

МИНОБРНАУКИ РОССИИ

Федеральное государственное бюджетное образовательное учреждение высшего образования «Горно-Алтайский государственный университет»
(ФГБОУ ВО ГАГУ, ГАГУ, Горно-Алтайский государственный университет)

Математические основы криптографии рабочая программа дисциплины (модуля)

Закреплена за кафедрой **кафедра математики, физики и информатики**

Учебный план 02.03.01_2022_622.plx
02.03.01 Математика и компьютерные науки
Цифровые технологии

Квалификация **бакалавр**

Форма обучения **очная**

Общая трудоемкость **3 ЗЕТ**

Часов по учебному плану	108	Виды контроля в семестрах:
в том числе:		зачеты 6
аудиторные занятия	36	
самостоятельная работа	62,1	
часов на контроль	8,85	

Распределение часов дисциплины по семестрам

Семестр (<Курс>.<Семестр на курсе>)	6 (3.2)		Итого	
	15 4/6			
Неделя	УП	РП	УП	РП
Лекции	18	18	18	18
Лабораторные	18	18	18	18
Консультации (для студента)	0,9	0,9	0,9	0,9
Контроль самостоятельной работы при проведении аттестации	0,15	0,15	0,15	0,15
Итого ауд.	36	36	36	36
Контактная работа	37,05	37,05	37,05	37,05
Сам. работа	62,1	62,1	62,1	62,1
Часы на контроль	8,85	8,85	8,85	8,85
Итого	108	108	108	108

Программу составил(и):

кандидат физико-математических наук, доцент, Кайгородов Евгений Владимирович

Рабочая программа дисциплины

Математические основы криптографии

разработана в соответствии с ФГОС:

Федеральный государственный образовательный стандарт высшего образования - бакалавриат по направлению подготовки 02.03.01 Математика и компьютерные науки (приказ Минобрнауки России от 23.08.2017 г. № 807)

составлена на основании учебного плана:

02.03.01 Математика и компьютерные науки

утвержденного учёным советом вуза от 27.01.2022 протокол № 1.

Рабочая программа утверждена на заседании кафедры

кафедра математики, физики и информатики

Протокол от 14.04.2022 протокол № 9

Зав. кафедрой Богданова Рада Александровна

Визирование РПД для исполнения в очередном учебном году

Рабочая программа пересмотрена, обсуждена и одобрена для
исполнения в 2024-2025 учебном году на заседании кафедры
кафедра математики, физики и информатики

Протокол от 11 ___04__ 2024 г. № 8
И. о. зав. кафедрой Богданова Рада Александровна

1. ЦЕЛИ И ЗАДАЧИ ОСВОЕНИЯ ДИСЦИПЛИНЫ

1.1	<i>Цели:</i> изложение основополагающих принципов защиты информации с помощью криптографических методов и примеров реализации этих методов на практике; изучение математических основ криптографии, истории развития криптографии, включая современные тенденции, основных алгоритмов шифрования и криптографических протоколов обмена информацией.
1.2	<i>Задачи:</i> изучение основных арифметических и алгебраических основ криптографии; изучение криптографических алгоритмов; знакомство с криптографическими методами современных криптосистем.

2. МЕСТО ДИСЦИПЛИНЫ В СТРУКТУРЕ ООП

Цикл (раздел) ООП:	
2.1	Требования к предварительной подготовке обучающегося:
2.1.1	Математический анализ
2.1.2	Алгебра
2.1.3	Теория чисел
2.2	Дисциплины и практики, для которых освоение данной дисциплины (модуля) необходимо как предшествующее:
2.2.1	Подготовка к процедуре защиты и защита выпускной квалификационной работы

3. КОМПЕТЕНЦИИ ОБУЧАЮЩЕГОСЯ, ФОРМИРУЕМЫЕ В РЕЗУЛЬТАТЕ ОСВОЕНИЯ ДИСЦИПЛИНЫ (МОДУЛЯ)

ОПК-1: Способен консультировать и использовать фундаментальные знания в области математического анализа, комплексного и функционального анализа алгебры, аналитической геометрии, дифференциальной геометрии и топологии, дифференциальных уравнений, дискретной математики и математической логики, теории вероятностей, математической статистики и случайных процессов, численных методов, теоретической механики в профессиональной деятельности	
ИД-1.ОПК-1: Знает основные понятия, определения, свойства математических объектов, формулировки и методы доказательств математических утверждений	
знать основные задачи и понятия криптографии;	
ИД-2.ОПК-1: Умеет доказывать утверждения, решать задачи в области математических наук	
уметь доказывать основные теоретико-числовые теоремы, пользоваться научно-технической литературой в области криптографии, применять отечественные и зарубежные стандарты в области криптографических методов компьютерной безопасности для проектирования, разработки и оценки защищенности компьютерных систем;	
ИД-3.ОПК-1: Способен консультировать в области фундаментальной математики	
владеть методикой построения, анализа и применения математических моделей для оценки степени защищенности информационной системы, качества использованных алгоритмов и технологий;	
ОПК-4: Способен находить, анализировать, реализовывать программно и использовать на практике математические алгоритмы, в том числе с применением современных вычислительных систем	
ИД-1.ОПК-4: Знает теоретические основы математических алгоритмов, особенности программной реализации математических алгоритмов, в том числе с применением современных вычислительных машин	
знать принципы построения криптографических алгоритмов, криптографические стандарты и их использование в информационных системах;	
ИД-2.ОПК-4: Умеет находить, анализировать, программно реализовывать математические алгоритмы, в том числе с применением современных вычислительных машин	
уметь использовать частотные характеристики открытых текстов для анализа простейших шифров замены и перестановки;	
ИД-3.ОПК-4: Владеет навыками использования на практике математических алгоритмов, реализованных с применением современных вычислительных машин	
владеть навыками использования типовых криптографических алгоритмов;	

4. СТРУКТУРА И СОДЕРЖАНИЕ ДИСЦИПЛИНЫ (МОДУЛЯ)							
Код занятия	Наименование разделов и тем /вид занятия/	Семестр / Курс	Часов	Компетенции	Литература	Инте ракт.	Примечание
	Раздел 1. Введение в криптографию						
1.1	Введение. История криптографии. Исторические шифры /Лек/	6	2	ИД-1.ОПК-1 ИД-2.ОПК-1 ИД-3.ОПК-1 ИД-1.ОПК-4 ИД-2.ОПК-4 ИД-3.ОПК-4	Л1.1 Л1.2Л2.1	1	проблемная лекция
1.2	Свойства информации. Ситуационные задачи на определение свойств информации, подлежащей криптографическому преобразованию. Исторические шифры и их криптоанализ. Компьютерная реализация и вскрытие шифров замены /Лаб/	6	2	ИД-1.ОПК-1 ИД-2.ОПК-1 ИД-3.ОПК-1 ИД-1.ОПК-4 ИД-2.ОПК-4 ИД-3.ОПК-4	Л1.1 Л1.2Л2.1	2	круглый стол
1.3	Введение. История криптографии. Исторические шифры /Ср/	6	11	ИД-1.ОПК-1 ИД-2.ОПК-1 ИД-3.ОПК-1 ИД-1.ОПК-4 ИД-2.ОПК-4 ИД-3.ОПК-4	Л1.1 Л1.2Л2.1	0	
	Раздел 2. Математическая формализация. Виды шифров						
2.1	Математическая модель шифра. Теория секретности Шеннона /Лек/	6	1	ИД-1.ОПК-1 ИД-2.ОПК-1 ИД-3.ОПК-1 ИД-1.ОПК-4 ИД-2.ОПК-4 ИД-3.ОПК-4	Л1.1 Л1.2Л2.1	1	лекция с запланированными ошибками
2.2	Блочные шифры /Лек/	6	2	ИД-1.ОПК-1 ИД-2.ОПК-1 ИД-3.ОПК-1 ИД-1.ОПК-4 ИД-2.ОПК-4 ИД-3.ОПК-4	Л1.1 Л1.2Л2.1	2	проблемная лекция
2.3	Псевдослучайные последовательности и поточные шифры /Лек/	6	2	ИД-1.ОПК-1 ИД-2.ОПК-1 ИД-3.ОПК-1 ИД-1.ОПК-4 ИД-2.ОПК-4 ИД-3.ОПК-4	Л1.1 Л1.2Л2.1	0	

2.4	Теория имитостойкости Симмонса и криптографические хэш-функции /Лек/	6	1	ИД-1.ОПК-1 ИД-2.ОПК-1 ИД-3.ОПК-1 ИД-1.ОПК-4 ИД-2.ОПК-4 ИД-4 ИД-3.ОПК-4	Л1.1 Л1.2Л2.1	0	
2.5	Асимметричные (с открытым ключом) шифры /Лек/	6	4	ИД-1.ОПК-1 ИД-2.ОПК-1 ИД-3.ОПК-1 ИД-1.ОПК-4 ИД-2.ОПК-4 ИД-4 ИД-3.ОПК-4	Л1.1 Л1.2Л2.1	2	проблемная лекция
2.6	Компьютерная реализация и вскрытие шифров перестановки и гаммирования. Построение моделей шифров /Лаб/	6	2	ИД-1.ОПК-1 ИД-2.ОПК-1 ИД-3.ОПК-1 ИД-1.ОПК-4 ИД-2.ОПК-4 ИД-4 ИД-3.ОПК-4	Л1.1 Л1.2Л2.1	2	круглый стол
2.7	Вероятностные характеристики текстов. Определение избыточности текста, языка. Вероятностные характеристики простых шифров. Расчет параметров шифров. Расстояние единственности, определение количества ложных ключей /Лаб/	6	2	ИД-1.ОПК-1 ИД-2.ОПК-1 ИД-3.ОПК-1 ИД-1.ОПК-4 ИД-2.ОПК-4 ИД-4 ИД-3.ОПК-4	Л1.1 Л1.2Л2.1	0	
2.8	Блочные шифры. ГОСТ 28147-89, IDEA и DES. Многочлены над Z_2 и блочный шифр AES /Лаб/	6	2	ИД-1.ОПК-1 ИД-2.ОПК-1 ИД-3.ОПК-1 ИД-1.ОПК-4 ИД-2.ОПК-4 ИД-4 ИД-3.ОПК-4	Л1.1 Л1.2Л2.1	2	кластер
2.9	Псевдослучайные генераторы на основе РСЛОС. Оценка свойств гаммы шифра. Изучение современных поточных криптосистем /Лаб/	6	2	ИД-1.ОПК-1 ИД-2.ОПК-1 ИД-3.ОПК-1 ИД-1.ОПК-4 ИД-2.ОПК-4 ИД-4 ИД-3.ОПК-4	Л1.1 Л1.2Л2.1	0	
2.10	Вычисление параметров имитостойкости, помехоустойчивости шифров. Построение криптографической хэш-функции на основе блочного шифра и исследование ее свойств методами математической статистики и теории информации /Лаб/	6	2	ИД-1.ОПК-1 ИД-2.ОПК-1 ИД-3.ОПК-1 ИД-1.ОПК-4 ИД-2.ОПК-4 ИД-4 ИД-3.ОПК-4	Л1.1 Л1.2Л2.1	2	кластер

2.11	Вычисления в Zn. Шифр с открытым ключом: RSA, Эль-Гамала, Шамира, Диффи-Хэллмана, Рабина, Гольдвассер-Микали, Блома-Гольдвассер, Меркла-Хэллмана. Генерация больших простых чисел для асимметричных криптосистем /Лаб/	6	2	ИД-1.ОПК-1 ИД-2.ОПК-1 ИД-3.ОПК-1 ИД-1.ОПК-4 ИД-2.ОПК-4 ИД-3.ОПК-4	Л1.1 Л1.2Л2.1	0	
2.12	Математическая модель шифра. Теория секретности Шеннона /Ср/	6	2	ИД-1.ОПК-1 ИД-2.ОПК-1 ИД-3.ОПК-1 ИД-1.ОПК-4 ИД-2.ОПК-4 ИД-3.ОПК-4	Л1.1 Л1.2Л2.1	0	
2.13	Блочные шифры /Ср/	6	6,1	ИД-1.ОПК-1 ИД-2.ОПК-1 ИД-3.ОПК-1 ИД-1.ОПК-4 ИД-2.ОПК-4 ИД-3.ОПК-4	Л1.1 Л1.2Л2.1	0	
2.14	Псевдослучайные последовательности и поточные шифры /Ср/	6	2	ИД-1.ОПК-1 ИД-2.ОПК-1 ИД-3.ОПК-1 ИД-1.ОПК-4 ИД-2.ОПК-4 ИД-3.ОПК-4	Л1.1 Л1.2Л2.1	0	
2.15	Теория имитостойкости Симмонса и криптографические хэш-функции /Ср/	6	2	ИД-1.ОПК-1 ИД-2.ОПК-1 ИД-3.ОПК-1 ИД-1.ОПК-4 ИД-2.ОПК-4 ИД-3.ОПК-4	Л1.1 Л1.2Л2.1	0	
2.16	Асимметричные (с открытым ключом) шифры /Ср/	6	13	ИД-1.ОПК-1 ИД-2.ОПК-1 ИД-3.ОПК-1 ИД-1.ОПК-4 ИД-2.ОПК-4 ИД-3.ОПК-4	Л1.1 Л1.2Л2.1	0	
	Раздел 3. Электронная цифровая подпись						
3.1	Схемы цифровой подписи /Лек/	6	2	ИД-1.ОПК-1 ИД-2.ОПК-1 ИД-3.ОПК-1 ИД-1.ОПК-4 ИД-2.ОПК-4 ИД-3.ОПК-4	Л1.1 Л1.2Л2.1	2	проблемная лекция

3.2	Эллиптические кривые над конечным полем. Шифры и ЭЦП на их основе /Лек/	6	2	ИД-1.ОПК-1 ИД-2.ОПК-1 ИД-3.ОПК-1 ИД-1.ОПК-4 ИД-2.ОПК-4 ИД-4 ИД-3.ОПК-4	Л1.1 Л1.2Л2.1	2	лекция- визуализация
3.3	Реализация схемы ЭЦП: RSA, Эль-Гамала и ее варианты, Фиата-Шамира, Онга-Шнорра-Шамира, Шнорра. Неотрицаемая подпись Шаума-ван-Антверпена. Эллиптические кривые над конечным полем. Преобразование криптосистемы над Z_p в криптосистему на эллиптической кривой /Лаб/	6	2	ИД-1.ОПК-1 ИД-2.ОПК-1 ИД-3.ОПК-1 ИД-1.ОПК-4 ИД-2.ОПК-4 ИД-4 ИД-3.ОПК-4	Л1.1 Л1.2Л2.1	0	
3.4	Схемы цифровой подписи /Ср/	6	11	ИД-1.ОПК-1 ИД-2.ОПК-1 ИД-3.ОПК-1 ИД-1.ОПК-4 ИД-2.ОПК-4 ИД-4 ИД-3.ОПК-4	Л1.1 Л1.2Л2.1	0	
3.5	Эллиптические кривые над конечным полем. Шифры и ЭЦП на их основе /Ср/	6	2	ИД-1.ОПК-1 ИД-2.ОПК-1 ИД-3.ОПК-1 ИД-1.ОПК-4 ИД-2.ОПК-4 ИД-4 ИД-3.ОПК-4	Л1.1 Л1.2Л2.1	0	
	Раздел 4. Криптографические протоколы						
4.1	Введение в криптографические протоколы /Лек/	6	2	ИД-1.ОПК-1 ИД-2.ОПК-1 ИД-3.ОПК-1 ИД-1.ОПК-4 ИД-2.ОПК-4 ИД-4 ИД-3.ОПК-4	Л1.1 Л1.2Л2.1	0	
4.2	Изучение примитивных протоколов. Изучение криптосистемы Kerberos /Лаб/	6	2	ИД-1.ОПК-1 ИД-2.ОПК-1 ИД-3.ОПК-1 ИД-1.ОПК-4 ИД-2.ОПК-4 ИД-4 ИД-3.ОПК-4	Л1.1 Л1.2Л2.1	0	
4.3	Введение в криптографические протоколы /Ср/	6	13	ИД-1.ОПК-1 ИД-2.ОПК-1 ИД-3.ОПК-1 ИД-1.ОПК-4 ИД-2.ОПК-4 ИД-4 ИД-3.ОПК-4	Л1.1 Л1.2Л2.1	0	
	Раздел 5. Консультации						

5.1	Консультация по дисциплине /Конс/	6	0,9	ИД-1.ОПК-1 ИД-2.ОПК-1 ИД-3.ОПК-1 ИД-1.ОПК-4 ИД-2.ОПК-4 ИД-3.ОПК-4	Л1.1 Л1.2Л2.1	0	
Раздел 6. Промежуточная аттестация (зачёт)							
6.1	Подготовка к зачёту /Зачёт/	6	8,85	ИД-1.ОПК-1 ИД-2.ОПК-1 ИД-3.ОПК-1 ИД-1.ОПК-4 ИД-2.ОПК-4 ИД-3.ОПК-4	Л1.1 Л1.2Л2.1	0	
6.2	Контактная работа /КСРАТ/	6	0,15	ИД-1.ОПК-1 ИД-2.ОПК-1 ИД-3.ОПК-1 ИД-1.ОПК-4 ИД-2.ОПК-4 ИД-3.ОПК-4	Л1.1 Л1.2Л2.1	0	

5. ФОНД ОЦЕНОЧНЫХ СРЕДСТВ

5.1. Контрольные вопросы и задания

Вопросы к зачету

1. Основные понятия и определения криптографии.
2. Виды криптосистем. Задачи, решаемые методами криптографии.
3. Виды информации, подлежащие закрытию, их модели и свойства. Частотные характеристики открытых сообщений. Критерии на открытый текст. Особенности нетекстовых сообщений.
4. История криптографии. Основные этапы становления науки криптографии.
5. Классификация шифров замены. Шифр Цезаря. Шифр простой замены. Шифр Плейфера. Полибианский квадрат. Шифр Хилла. Шифр Виженера. Частотный анализ. Тест Казиски.
6. Классификация шифров перестановки. Примеры шифров перестановки и их криптоанализ.
7. Шифры гаммирования. Шифр Вернама. Подходы к его криптоанализу.
8. Композиции шифров. Enigma. Шифр Хейглина.
9. Математическая модель шифра.
10. Атаки и угрозы шифрам.
11. Блочные шифры и их ключевая система. Замены и перестановки.
12. Сеть Фейстеля. Шифры DES, ГОСТ 28147-89.
13. Шифр AES
14. Шифр IDEA.
15. Подходы к криптоанализу блочных шифров. Дифференциальный криптоанализ. Линейный криптоанализ.
16. Режимы шифрования.
17. Многократное шифрование. Композиция блочных шифров.
18. Совершенные шифры. Пример совершенного шифра.
19. Энтропийные характеристики шифров. Идеальные шифры.
20. Избыточность языка.
21. Оценка числа ложных ключей и расстояние единственности.
22. Безусловно стойкие и вычислительно стойкие шифры.
23. Псевдослучайные последовательности (ПСП). Характеристики генераторов ПСП (ПСГ). Требования к криптографическим ПСП. Примеры ПСГ и криптографических ПСГ.
24. Поточные шифры. Общая схема поточного шифра. Синхронные и самосинхронизирующиеся шифры.
25. Регистры сдвига с обратной линейной связью (РСЛОС).
26. ПСГ на основе РСЛОС.
27. Шифр A5.
28. Нелинейные регистры сдвига.

29. Шифр RC4.
30. Теория имитостойкости Симмонса. Имитация и подмена сообщения. Характеристики имитостойкости. Совершенная имитостойкость.
31. Коды аутентификации сообщений.
32. Защитные контрольные суммы.
33. Криптографические хэш-функции и требования к ним.
34. Подходы к проектированию хэш-функций.
35. Хэш-функции на основе блочного шифра.
36. Ключевые хэш-функции.
37. Понятие односторонней функции и односторонней функции с "лазейкой". Проблемы факторизации целых чисел и логарифмирования в конечных полях.
38. Криптосистема Диффи-Хэллмана. Пример.
39. Криптосистема RSA. Пример.
40. Криптосистема Эль-Гамала. Пример.
41. Криптосистема Рабина. Пример.
42. Криптосистема Гольдвассер-Микали. Пример.
43. Криптосистема Блюма-Гольдвассер. Пример.
44. Рюкзачные шифры. Криптосистема Меркла-Хэллмана.
45. Понятие электронной цифровой подписи и требования к ней. Атаки и угрозы схемам ЭЦП.
46. Подпись RSA, Эль-Гамала.
47. Подпись Фиата-Шамира.
48. Подпись Онга-Шнорра-Шамира.
49. Неотрицаемая подпись Шаума-ван-Антверпена.
50. Стандарты ЭЦП: DSS, ГОСТ Р 34.10-94.
51. Эллиптическая кривая над конечным полем. Операции на эллиптической кривой. Сумма точек. Кратная точка.
52. Проблема дискретного логарифмирования на эллиптической кривой. Переход от шифра (ЭЦП) в Z_p к шифру (ЭЦП) на эллиптической кривой.
53. Шифр Эль-Гамала на эллиптической кривой.
54. Стандарты ЭЦП на эллиптической кривой: ГОСТ Р 34.10-2001, ECDSA.

5.2. Темы письменных работ

5.3. Фонд оценочных средств

Формируется отдельным документом в соответствии с Положением о фонде оценочных средств в Горно-Алтайском

5.4. Перечень видов оценочных средств

стр. 10

6. УЧЕБНО-МЕТОДИЧЕСКОЕ И ИНФОРМАЦИОННОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ (МОДУЛЯ)

6.1. Рекомендуемая литература

6.1.1. Основная литература

	Авторы, составители	Заглавие	Издательство, год	Эл. адрес
Л1.1	Тебуева Ф.Б., Антонов В.О.	Теоретико-числовые методы в криптографии: учебное пособие : электронный учебник	Ставрополь : Северо-Кавказский федеральный	http://www.iprbookshop.ru/75601.html
Л1.2	Басалова Г.В.	Основы криптографии: учебное пособие	Москва: Интернет-Университет Информационных Технологий (ИНТУИТ), Ай Пи Ар Медиа, 2024	https://www.iprbookshop.ru/133959.html

6.1.2. Дополнительная литература

	Авторы, составители	Заглавие	Издательство, год	Эл. адрес
Л2.1	Кирпичников А.П., Хайбуллина З.М.	Криптографические методы защиты компьютерной информации: учебное пособие	Казань: Казанский национальный исследовательский технологический университет, 2016	http://www.iprbookshop.ru/79313.html

6.3.1 Перечень программного обеспечения

6.3.1.1	Яндекс.Браузер
6.3.1.2	Kaspersky Endpoint Security для бизнеса СТАНДАРТНЫЙ
6.3.1.3	MS Office
6.3.1.4	NVDA
6.3.1.5	РЕД ОС
6.3.1.6	LibreOffice
6.3.1.7	MS Windows
6.3.2 Перечень информационных справочных систем	
6.3.2.1	Электронно-библиотечная система IPRbooks
6.3.2.2	База данных «Электронная библиотека Горно-Алтайского государственного университета»

7. ОБРАЗОВАТЕЛЬНЫЕ ТЕХНОЛОГИИ

	проблемная лекция	
	лекция-визуализация	
	кластер	
	лекция с запланированными ошибками	
	круглый стол	

8. МАТЕРИАЛЬНО-ТЕХНИЧЕСКОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ (МОДУЛЯ)

Номер аудитории	Назначение	Основное оснащение
207 Б1	Учебная аудитория для проведения занятий лекционного типа, занятий семинарского типа, курсового проектирования (выполнения курсовых работ), групповых и индивидуальных консультаций, текущего контроля и промежуточной аттестации	Ученическая доска, мультимедиапроектор, экран, компьютер. Рабочее место преподавателя, посадочные места обучающихся (по количеству обучающихся), кафедра
209 Б1	Компьютерный класс. Учебная аудитория для проведения занятий лекционного типа, занятий семинарского типа, курсового проектирования (выполнения курсовых работ), групповых и индивидуальных консультаций, текущего контроля и промежуточной аттестации. Помещение для самостоятельной работы	Маркерная ученическая доска, экран, мультимедиапроектор, посадочные места обучающихся (по количеству обучающихся), рабочее место преподавателя, компьютеры с доступом в Интернет
211 Б1	Компьютерный класс. Учебная аудитория для проведения занятий лекционного типа, занятий семинарского типа, курсового проектирования (выполнения курсовых работ), групповых и индивидуальных консультаций, текущего контроля и промежуточной аттестации. Помещение для самостоятельной работы	Рабочее место преподавателя. Посадочные места обучающихся (по количеству обучающихся), компьютеры с доступом к Интернет

9. МЕТОДИЧЕСКИЕ УКАЗАНИЯ ДЛЯ ОБУЧАЮЩИХСЯ ПО ОСВОЕНИЮ ДИСЦИПЛИНЫ (МОДУЛЯ)**1. КАЛЕНДАРНЫЙ ПЛАН**

Календарный план вывешивается в лабораториях или лекционной аудитории и содержит информацию о распределении занятий по неделям, числе учебных часов, формах и времени контроля и пр.

В связи с праздниками и по другим причинам часть практических (лабораторных) занятий может исключаться или объединяться. Все возможные изменения укажет преподаватель в ходе занятий.

2. ВЫПОЛНЕНИЕ ПРАКТИЧЕСКИХ (ЛАБОРАТОРНЫХ) ЗАНЯТИЙ

Осмысленное решение задач невозможно без знания важнейших понятий, формул, законов и пр. данной темы. Поэтому

перед каждым практическим (лабораторным) занятием студенты должны переписать в классную тетрадь или на отдельные листы список таких понятий и формул с расшифровкой каждого понятия, формулировками всех теорем, смыслом каждого значка: не просто переписать слова "логарифмическое дифференцирование", а дать определение логарифмического дифференцирования; не просто написать "закон распределения дискретной случайной величины", а дать его формулировку и привести примеры; нужны не слова "плотность распределения", а график этой плотности распределения.

Большинство формул и понятий каждого списка будут важнейшими и в масштабах всего курса, т.е. должны быть заучены; при подготовке к практическому (лабораторному) занятию, однако, такой цели-максимум можно не ставить, ограничившись свободной ориентировкой в собственных записях. Преподаватель в начале занятия проверяет наличие и качество раскрытия содержания списка у каждого студента, причём НА ВСЕХ ЗАНЯТИЯХ без исключения, начиная с первого. Это и понятно: отсутствие списка или формальная его переписка — гарантия неэффективной работы студента на занятии. Одновременно проверяется решение домашних задач, которые должны быть распределены по занятиям и аккуратно пронумерованы с ПОЛНОЙ ЗАПИСЬЮ УСЛОВИЙ каждой задачи в отдельную тетрадь для домашних работ. Жалеть время на переписку условий не следует: это не только делает студента независимым от задачников, которых в нужный момент — на контрольной, зачёте — не окажется под рукой, но и помогает в решении задач, заставляя заметить какую-нибудь важную "мелочь" типа отсутствия начальных или краевых условий. Если при всем старании решить домашние задачи не удалось, ДОЛЖЕН БЫТЬ ПРЕДЪЯВЛЕН ЧЕРНОВИК РЕШЕНИЙ. Не имеющие без уважительной причины списка понятий и не приступавшие к решению домашних задач получают неудовлетворительную оценку и должны будут явиться на вызывную консультацию в часы ИРС. Разумеется, она открыта и для всех желающих.

Такие консультации проводятся регулярно с указанием времени в календарном плане. О веской причине предстоящей неявки студент-задолжник обязан заранее предупредить преподавателя; не оговоренная заранее неявка задолжника на вызывную консультацию влечёт ОБЯЗАТЕЛЬНОЕ ДОБАВОЧНОЕ ИНДИВИДУАЛЬНОЕ ЗАДАНИЕ — задачи, проработку конспекта и пр. Ясно, что при повторяющихся неявках на вызывные консультации студент ставит себя в очень сложное положение.

Если занятие было по ЛЮБЫМ причинам пропущено, следует, переписав у товарищей классные задачи и РАЗОБРАВШИСЬ В НИХ, подготовить список понятий, решить домашние задачи и явиться на ближайшую консультацию, где преподаватель проверит качество работы. Если причина пропуска уважительна, список надо лишь показать, а вот если нет — сдать, предварительно заучив.

ВНИМАНИЕ! Пропуск (по любой причине!) большого числа занятий, а тем более неявка на вызывные консультации означает, что преподавателю придётся затратить на работу с Вами значительное время: просмотреть по каждой теме переписанные классные задачи, проверить или принять списки понятий, проверить решение домашних и дополнительных задач. Если это происходит в середине семестра, то всё может окончиться благополучно — тут уж дело за Вашей добросовестностью и способностями. Но к концу семестра не поможет и добросовестность просто потому, что Вам не хватит времени: в первую очередь на консультациях, зачёте и пр. преподаватель будет работать со студентами без задолженности или с меньшей задолженностью. Как только закончились занятия, преподаватель НЕ ОБЯЗАН с Вами работать; с ним надо договариваться о каждой встрече, что зависит не только от Вашей готовности, но и его желания, мнения о Вас, занятости и пр. ИЗ-ЗА ПРОПУСКА БОЛЬШОГО ЧИСЛА ПРАКТИЧЕСКИХ (ЛАБОРАТОРНЫХ) ЗАНЯТИЙ ТАКЖЕ НЕСКОЛЬКО СТУДЕНТОВ ЕЖЕГОДНО ОТЧИСЛЯЮТСЯ ИЗ УНИВЕРСИТЕТА.

Замечу, что при проведении контрольных работ эффективно можно использовать только СВОИ списки понятий, классные и домашние тетради с задачами. Задачи контрольных подбираются однотипными с решавшимися дома и в аудитории, так что некачественной проработкой своих записей или их неполнотой нерадивый накажет сам себя.

ВНИМАНИЕ! Из многолетнего опыта успешного решения учебных задач мною извлечены лишь 3 универсальных истины для тех, кто также хотел бы научиться решать учебные задачи.

а) **ЗНАЙ ТЕОРИЮ И, ГЛАВНОЕ, ФОРМУЛЫ** (или хотя бы знай, где эти формулы найти). Если в задаче идёт речь о касательной и нормали к кривой, а ты не знаешь, что это такое и не помнишь геометрический смысл производной — дело безнадежно, т.к. ты даже не знаешь, где и что искать. Но если и знаешь, нужна оптимальная стратегия решения. Поэтому

б) **РЕШАЙ С КОНЦА**. Это значит: внимательно прочитай условия, сделав их полную математическую запись (не упуская ни одной «мелочи» типа пределов интегрирования, дифференциалов, правильных обозначений для всех величин, записи числовых значений в одной системе и пр.), определи, что надо найти — и с учетом условий задачи ПОДБЕРИ ФОРМУЛУ, КУДА ВХОДИТ ИСКОМАЯ ВЕЛИЧИНА. Правильно поставленный вопрос — половина решения. В простейших задачах нужна всего одна формула, в более сложных — ряд взаимосвязанных. Выбор этих формул — дело творческое, требующее не только знаний, но и опыта. Поэтому

в) **РЕШИ МНОГО ЗАДАЧ**. Если ты в своей жизни решил всего 2 математические задачи, то 3-ю скорее всего не решишь; если 2002, то 2003-ю скорее всего решишь. Лучше решать самому — хорошо запоминается, способствует самоуважению и усвоению теоретического материала, но годится решение преподавателя, товарища, из книжки — лишь бы решение запомнилось. При решении олимпиадных задач очень часто нужно знать какой-то специальный прием, сразу видеть, на какую теорему или закон дана задача.

К сожалению, эти истины непригодны при решении задач научных (не говоря уже о житейских): здесь чаще всего неизвестно не только как решать, но и что искать, каковы исходные данные, полны ли они, недостаточны или избыточны...

По итогам занятий на зачет (экзамен) выносятся 2 оценки: за умение решать задачи (по итогам контрольных и решению домашних задач) и за добросовестность (своевременность и качество работы со списками, пропуски занятий и т.д.).

ВНИМАНИЕ! Практические (лабораторные) занятия зачтены, если: а) есть полные списки понятий по всем темам, б) решены все домашние задачи, в) восстановлены все пропущенные занятия и сданы задолженности, г) зачтены все контрольные работы и индивидуальные задания.

3. ИЗУЧЕНИЕ ТЕОРЕТИЧЕСКОГО МАТЕРИАЛА

Практические умения и навыки могут быть получены только на прочной базе знаний, приобретенных при изучении теоретического материала. Но в основе знаний обязательно лежит процесс ЗАПОМИНАНИЯ, ЗАУЧИВАНИЯ. Действительно, любая область человеческих знаний — математика, физика, педагогика, медицина — опирается на определённый набор понятий ("производная — это...", "педагогика — это...", "электрический ток — это..."), фактов и явлений ("Волга впадает в Каспийское море", "одноименные заряды отталкиваются", "первым признаком заболевания дизентерией является..."), законов, теорем и закономерностей ("заряд в замкнутой системе сохраняется", "квадрат гипотенузы равен сумме квадратов катетов", "приём аспирина способствует снижению температуры больного"), использует собственные графические и символичные средства (чертежи, карты, формулы, схемы); и всё это надо заучить, запомнить, узнать желающему изучить данную науку. Не надо путать зубрёжку и заучивание: в первом случае смысл запоминаемого неизвестен, как в детской считалке "Энебенераба...", так что заучивание теоремы Пифагора не будет зубрёжкой, если осмыслены и заучены понятия "прямоугольный треугольник", "катет", "гипотенуза", "квадрат", "сумма". Вопрос о понимании, осмысливании материала достаточно сложен, чтобы на нём здесь останавливаться; важно, что проработка, осмысливание, понимание нового опирается на уже заученное, усвоенное знание. Не изучавшему английский язык фраза "Ай спик рашн" так же непонятна, как не изучавшему математику — "модуль смешанного произведения трех векторов численно равен значению объема параллелепипеда, построенного на этих векторах". Очень часто студент заявляет, что он со школы НЕ ПОНИМАЕТ математику, а на деле оказывается, что он её НЕ ЗНАЕТ; не помнит (или помнит примерно), что такое аргумент, функция, предел; не заучил, какими буквами обозначаются эти величины и как эти буквы пишутся и читаются. И если в данный момент студент НЕ ПОМНИТ, что такое первообразная или дифференциал, то причём здесь понимание? МАТЕМАТИКУ НАДО УЧИТЬ НАИЗУСТЬ, как иностранный язык: по десять понятий, формул, обозначений каждый день, по несколько раз, пока не запомнишь — и через год-два РЕГУЛЯРНЫХ ЗАНЯТИЙ заговоришь. УЧЕБА ПО НАСТОЯЩЕМУ — ЭТО ТЯЖЁЛЫЙ ТРУД, и ничего не добьются те, кто мечтает "понимать" математику без ежедневного труда по её ИЗУЧЕНИЮ. Корень учения горек, но плоды его (пока хотя бы в виде заслуженной пятёрки на экзамене) сладки.

"Но это сколько же надо заучивать, у нас не одна Ваша дисциплина!" — скажут иные студенты. Доля истины здесь есть, поэтому в университете и существуют преподаватели: они в соответствии с программами отбирают материал и организуют изучение, выделяя важнейшее, помогая и контролируя. Опытный преподаватель знает, что ВАЖНЕЙШИХ понятий, формул, явлений, законов, опытов, схем, графиков, констант за семестр сообщается студентам сотни две-три, и заучить их по силам даже тому, кто ничего не помнит (невероятный случай!) со школы — было бы желание. Рецепт прост: запиши это важнейшее несколько раз (моторная память самая прочная — кто научился ездить на велосипеде, ездит всю жизнь); проговори вслух и послушай товарища (используй слуховую память), подчеркни красной пастой, обведи рамочкой и внимательно рассмотри (зрительная память самая ёмкая — говорят же, что лучше один раз увидеть, чем сто раз услышать). Для облегчения студенческого труда всё важнейшее, что требует заучивания наизусть, выделяется преподавателем в ходе чтения лекции в рамку.

Однако будущему специалисту мало знать предмет, надо ещё уметь его излагать, объяснять другим, ибо среди людей живем, зачастую — менее опытных. В общем-то это искусство, которым овладевают всю жизнь, сплав знаний и ОПЫТА человека (недаром со временем специалисту начинают платить больше). Но в основе лежит, на мой взгляд, приобретаемое при изучении и в ходе работы умение видеть и излагать свой предмет как СИСТЕМУ знаний, а не набор отдельных заученных фактов. Для этого надо ПОМНИТЬ не только сами факты, но и связи между ними, их последовательность во времени, степень важности и сложности для восприятия, использование в дальнейшем курсе, необходимость свободного владения, силу эмоционального воздействия и т.д. и т.п. Время на изложение материала, как и время ответа школьника или студента, всегда ограничено; значит, надо помнить и распределение времени с учётом возможных вопросов, да ещё и уметь на ходу перестраиваться в случае каких-то непредвиденных обстоятельств (погас свет; не получилась демонстрация, на которую опиралось изложение нового материала, и пр.). Каждый из нас помнит со времен школы молодых учителей или практикантов, которые непонятно объясняют, постоянно заглядывая в тетрадку, а то и читая по ней; которые тихо и невнятно говорят и мелко пишут на доске; у которых постоянно не хватает времени и урок заканчивается фразой "Остальное посмотрите дома сами по учебнику". Всё это еще придётся испытать на себе почти каждому студенту в ходе практики; а пока ни слова не говорилось об умении владеть собой в присутствии на уроке проверяющего, видеть по реакции аудитории степень заинтересованности и понимания, не говорилось об искусстве интересно преподнести самый "сухой" материал и о проблеме проблем — умении поддержать дисциплину на уроке. УМЕНИЕ — ЭТО ЗНАНИЕ В ДЕЙСТВИИ. Значит, если хочешь уметь излагать материал, нужно постоянно пробовать это делать, использовать любую возможность: для самого себя, вслух или на бумаге; для товарищей на вечере, собрании, в комнате общежития, перед занятием; для преподавателя на практических (лабораторных) занятиях, в ходе теоретического собеседования, на коллоквиуме или экзамене. Можно продолжить аналогию с изучением иностранного языка: мало запомнить, как пишутся, читаются и произносятся слова; нужно ещё знать правила этого языка и обязательно в нём практиковаться, используя любую возможность. Лишь тогда будут понятны вопросы преподавателя и в ответ не выговорятся исковерканные фразы "Метод Гаусса — это когда...", "Матрица — это совокупность данных" или "Применяем подстановку Чебышева".

Кстати, аналогия с иностранным языком имеет и прямой смысл: в математике множество понятий обозначается словами иностранных языков, в основном латинского и греческого. Детерминант, система, дивергенция, ротор, вектор, матрица, интеграл, сумма и др. — нам их приходится заучивать, а итальянцу или англичанину они знакомы с детства как слова родного языка. То же с обозначениями: все без исключения математические величины имеют меру, эталон для сравнения, единицу измерения (в этом заслуга многих поколений математиков; а может ли медицина ИЗМЕРИТЬ тяжесть болезни, педагогика — степень мастерства учителя, а психология — силу эмоций?), требуя какой-то буквы для описания количества каждой такой величины. Эти буквы заимствованы в основном из латыни — языка международного общения учёных в пору становления математики как науки. Математикам ещё ничего, а какково медикам или биологам — заучивать названия всех болезней, костей, мышц, лекарств, растений, насекомых на латыни? Вот где зубрёжка!

Итак, важным компонентом профессионализма специалиста (а тем более, родителя или учителя) является, кроме отличного владения фактическим материалом, умение отобрать данные для конкретного разговора, беседы, расположить всё в нужной последовательности, выделить важнейшее, распределить время и пр. Всё это необходимо сделать до разговора и, в идеале, запомнить, что начнётся она с опроса Вани и Саши, затем Ваня решает домашнюю задачу, и на пятнадцатой минуте объяснение темы "Геометрические приложения определенного интеграла" надо начать не с повторения определения такого интеграла, а с просьбы представить себе жизнь без расчетов площадей, работы, сил, технических потребностей. На практике так не получается — слишком многое надо запоминать, поэтому все педагоги пишут ПЛАНЫ ЗАНЯТИЙ, где отобранный материал расположен в должной последовательности и примерно распределён по времени, где выделены формулы и понятия для записи обучаемыми, где сделаны какие-то важные для учителя пометки. Студентам на практике и начинающим учителям ЗАПРЕЩЕНО вести уроки, не имея предварительно составленных планов, т.к. их наличие — всё же гарантия, хотя и неполная, подготовки к занятию. План не только организует самого учителя, разгружает его память, позволяет накапливать материал и через год не начинать подготовку к занятию с нуля, но и служит мощной психологической поддержкой в ходе изложения новой темы; если что-то забыл, напутал, не сходится ответ в задаче — можно заглянуть в план. Правда, для начинающих здесь кроется опасность чрезмерной привязанности к плану, боязнь оторваться от него; а самые неумелые или ленивые просто-напросто ЧИТАЮТ записи вслух (речь не идет, конечно, о какой-то нужной цитате или отрывке произведения). Кроме того, подготовка качественного плана — отбор и запись материала, запоминание всего важного, прорешивание задач, подготовка эксперимента — требует поначалу большого времени, так что первые два-три года работы очень трудны, даже если забыть проблемы неумения поддержать дисциплину, вести классное руководство, говорить с родителями, быть точным и обязательным, проблемы вхождения в коллектив, бытовые, семейные и пр. и пр. Ведь планы-то нужны к каждому уроку! Ясно, что умению составлять такие планы также надо тщательно учиться в университете.

Поэтому в предложенном курсе изучение теоретического материала строится на базе ПЛАНОВ ОТВЕТОВ (ДАЙДЖЕСТОВ), куда в сжатом виде входит материал лекций в нужной последовательности, причем важнейшие понятия, формулы, теоремы и пр., которые следует заучить наизусть, лишь упоминаются, а вот весь вспомогательный материал (математические выкладки, схемы, рисунки) приводится более подробно. Дайджесты собираются студентом самостоятельно после разъяснений преподавателя в начале курса. От студента требуется ПОДГОТОВИТЬСЯ К ИХ ИСПОЛЬЗОВАНИЮ ПРИ ОТВЕТЕ; переписать план ответа на отдельный листок желательно (включается память!), но не обязательно. Подготовка означает не только заучивание всего, что надо заучить, но и готовность развернуть дайджест в виде подробного и полного ответа, раскрыть математические связи в промежуточных выкладках, указать смысл каждого значка, буквы, рисунка, верно назвать все буквы и т.д. План ответа — не догма, а руководство к действию. Да, следование плану навязывает студенту определённую логику ответа, за которой стоят искусство и опыт специалиста (читай — учителя или родителя). Но можно подготовить свой план, следовать своей логике или логике учебника — лишь бы план включал весь материал дайджеста. Дайджест — узаконенная подсказка, где материал целой лекции занимает полстраницы, так что свободное владение дайджестом — уже хороший признак. Дайджест ограничивает и требования преподавателя: за рамки плана ответа его вопросы выходить не должны.

Часть материала нужно изучить самостоятельно, что предполагает подготовку своего плана ответа. **ВНИМАНИЕ!** Это должен быть ПЛАН, А НЕ ТЕКСТ ответа, который просто зачитывается. Чтение заготовленного дома текста совершенно недопустимо! Такая форма работы с учебником возможна при первой проработке материала для себя, но изложение его оценивающему ответ преподавателю требует гораздо более плотной свёртки информации в памяти.

Составление и проработка планов ответа не только готовят студента к будущей профессиональной деятельности, но и разгружают его память за счёт вспомогательного материала, промежуточных математических выкладок и пр., концентрируя внимание на основном. Дайджесты определяют тот объём ответа, которого ожидает преподаватель, причём он вправе требовать глубокого усвоения всего материала дайджеста (в том числе и вывода формул, т.к. запоминать вывод не надо). Разумеется, студент может использовать любой дополнительный к дайджесту материал.

Ясно, что неполный или некачественно проработанный план ответа гарантирует снижение оценки. Это следует из тех простых соображений, что каждый дайджест включает материал примерно одной лекции, т.е. на подготовку и проработку его надо затратить 2-3 часа — труд немалый и непростой, требующий использования всех видов памяти, изучения конспекта лекций и учебников, дополнительной литературы. И если этих часов интенсивной работы не было, дайджест принесёт мало пользы. Качество подготовки, т.е. умение свободно и правильно говорить на МАТЕМАТИЧЕСКОМ ЯЗЫКЕ, будет проверяться в ходе теоретического собеседования в кабинете, на коллоквиумах и на зачете (экзамене).

Фактический материал для части дайджестов не удастся найти в учебниках по той простой причине, что он туда ещё не успел попасть. Это также одна из проблем преподавания, особенно острая из-за быстрого развития современной науки:

часть знаний постоянно приходится обновлять и пополнять. Представителям математики и естественных дисциплин — физикам, химикам, биологам — в сравнении с преподавателями общественных и гуманитарных дисциплин приходится работать гораздо меньше, т.к. основная часть их теоретического багажа не устареет никогда: пока существует наша Вселенная, в ней будут верны теорема Лагранжа, законы Ньютона, периодическая система Менделеева, уравнения Максвелла и законы наследственности. Помочь в обновлении знаний призваны научно-популярные журналы «Квант», «Наука и жизнь», «Техника — молодёжи», «Знание — сила», «В мире науки» и другие, оперативно публикующие информацию о новейших достижениях науки и техники. К сожалению, практика показывает, что многие наши студенты и не подозревают о существовании таких журналов, не говоря уже о регулярном их чтении. Они ещё не знают, что достаточно преподавателю несколько раз не ответить на вопросы любознательных учеников о кривизне пространства, возможности деления на ноль, логических парадоксах и софизмах или возможности путешествия во времени с помощью туннелей в пространстве — и с мечтой об авторитете придётся надолго, если не навсегда, проститься.

Итак, при изучении теоретического материала действуй так.

- а) Серьёзно настройся на ЗАУЧИВАНИЕ важнейшего материала, выделенного преподавателем на лекциях. Используй все виды памяти, не забывая главного: повторение — мать учения, а регулярную работу (по 10 понятий и формул КАЖДЫЙ день) не заменит никакой штurm перед экзаменом.
- б) Учись говорить на ПРАВИЛЬНОМ математическом языке. Заучи, какими буквами обозначаются величины в курсе, как эти буквы пишутся и читаются. Правильно произноси фамилии ученых. Не забывай единицы всех величин, значения ряда констант.
- в) Учись ГРАМОТНО излагать материал. Основное оружие человека — слово. А много ли приходится школьнику говорить на уроках? По подсчетам В. Ф. Шаталова — в лучшем случае 2 минуты в день. И вот этот «молчаливый» школьник поступает в университет. Здесь возможностей может быть еще меньше — лекции, практические и лабораторные занятия могут быть организованы так (хотя это, на мой взгляд, неверно), что за семестр студент вообще ни разу не побеседует с преподавателем. А как такой человек будет работать в школе или вузе, да и вообще среди людей, себе подобных? Поэтому постоянно читай литературу и конспекты лекций (много читающие люди не помнят правил родного языка, но правильно говорят и пишут); внимательно слушай речь преподавателей, стараясь не пропустить ни единого занятия; слушай ответы товарищей и запоминай их ошибки — но самое главное, используй любую возможность потренироваться в изложении материала на ИРС, консультации, практическом (лабораторном) занятии, в лаборатории, на коллоквиуме, для соседа по общежитию, перед зеркалом и т.д. и т.п.
- г) Работай РЕГУЛЯРНО. Перед новой лекцией просмотри материал предыдущей; сразу выясни все непонятное на консультации, в учебнике или у товарищей. Не оставляй подготовку планов ответа и проработку самостоятельного материала, особенно по научно-популярной литературе, на потом: одного дня перед зачетом (экзаменом) всегда не хватает, а проработка таких тем требует длительных поисков в библиотеках многих научно-популярных журналов.

4. САМОСТОЯТЕЛЬНАЯ РАБОТА

Высшая школа отличается от средней не только специализацией подготовки, но главным образом методикой учебной работы, степенью самостоятельности студентов. Преподаватель лишь определенным образом организует познавательную деятельность студентов, само же познание осуществляет САМ СТУДЕНТ.

Самостоятельная работа прежде всего завершает задачи всех других видов учебной работы. **ВНИМАНИЕ! НИКАКИЕ ЗНАНИЯ, НЕ СТАВШИЕ ОБЪЕКТОМ СОБСТВЕННОЙ ДЕЯТЕЛЬНОСТИ, НЕ МОГУТ СЧИТАТЬСЯ ПОДЛИННЫМ ДОСТОЯНИЕМ ЧЕЛОВЕКА.** Помимо практической важности самостоятельная работа имеет большое воспитательное значение: она формирует самостоятельность не только как совокупность определенных умений и навыков, но и как черту характера, играющую существенную роль в структуре личности современного специалиста высшей квалификации.

Однако же, самостоятельная работа часто игнорируется студентами в течение семестра, что совершенно недопустимо. Появляется соблазн сначала "погулять", а потом "поднажать".

ВНИМАНИЕ! Эта ситуация является стандартной ловушкой, из-за которой ежегодно несколько человек отчисляются из университета! Дело в том, что объём работы по математическим дисциплинам велик, а число занятий ограничено (см. календарный план), причем по окончании курса ПРЕПОДАВАТЕЛЬ НЕ ОБЯЗАН С ВАМИ РАБОТАТЬ (см. выше). А не сданы домашние, контрольные и индивидуальные работы — учебный план не выполнен, и о сдаче зачета (экзамена) и речи быть не может! Поэтому действуй так:

1. За **НЕСКОЛЬКО** дней до лекции или практического (лабораторного) занятия (не в последний день, т.к. это гарантирует неготовность!) в часы самоподготовки, необходимо прочитать предыдущую лекцию, **РАЗОБРАВШИСЬ** с основными понятиями, теоремами и логической структурой лекции (а не механически, зубря формулировки!).
2. **ЗАГОДЯ** научись решать простейшие базовые задачи, приведенные в лекции. Систематически **ОБЪЯСНЯЙ** себе (товарищу, соседу, зеркалу) каждый свой шаг при решении, больше говори, меньше записывай. То же правило применяй при решении домашних, контрольных и индивидуальных заданий.
3. При подготовке к теоретическому собеседованию (коллоквиуму) дома готовятся ответы на все вопросы, но отвечать

каждый студент будет лишь часть их, указанную преподавателем. Подготовка к собеседованию требует нескольких дней! Собеседование идет за столом преподавателя, и студенту нужна лишь чистая бумага. Пользоваться учебником или конспектом здесь запрещено.

Можно, однако, подготовить сжатый ПЛАН ОТВЕТА (дайджест), куда включаются промежуточные математические выкладки, рисунки, графики и т.п.: важнейшие формулы, понятия и т.д., которые следует знать наизусть (они выделяются преподавателем на лекции), должны быть указаны в планах ответов БЕЗ РАСКРЫТИЯ СОДЕРЖАНИЯ.

Ответ строится в форме связного изложения теоретического материала с помощью планов ответов. В ходе ответа студенты обязаны внимательно слушать друг друга и преподавателя — учиться лучше на чужих ошибках! — но не подсказывать, т.к. оценка за собеседование ставится и в конце его объявляется каждому, существенно влияя на экзаменационную оценку (а в случае подсказки надо эту оценку делить на двоих!). Если один из студентов не прошёл собеседование, то сдающие с ним коллоквиум, ответив на свои вопросы, все же НЕ БУДУТ, как правило, допущены до зачета (экзамена), пока не помогут товарищу подготовиться и пройти собеседование. Это объясняется тем, что на зачет (экзамен) будут выноситься ВСЕ вопросы к собеседованиям, и любому студенту могут попасть как раз те вопросы, которые не были разобраны с преподавателем. На обстоятельное теоретическое собеседование, главная цель которого — дать возможность КАЖДОМУ студенту потренироваться в изложении материала — требуется 15-20 минут на студента. Повторные, на данном занятии, собеседования возможны после сдачи теории всеми остальными студентами; это реально, если надо лишь досдать какую-то малую часть теоретического вопроса. Студенты, по ЛЮБЫМ причинам пропустившие коллоквиум, не сдавшие теорию, не выполнившие индивидуальные задания и не ответившие на дополнительные вопросы — считаются задолжниками и должны восполнить отставание во время вызывных консультаций: ВСЕ пропущенные часы, как правило, должны быть восстановлены.

Как правило, за одну беседу студент должен сдать коллоквиум и/или защитить индивидуальную (контрольную) работу. Это вполне реально, если подготовка была добросовестной: до 15 мин — на теоретическое собеседование, несколько минут — на обоснование выкладок в предъявленных решенных задачах. Но если предварительно не были потрачены часы на подготовку обоснования решения, а главное, теоретического собеседования — ЗАДОЛЖЕННОСТЬ ГАРАНТИРОВАНА! Сдав данный коллоквиум, следует готовиться к следующей беседе (с № 1 — на № 2, и т.д.). По итогам работы в семестре на экзамен могут выноситься три оценки: за теоретические знания, показанные в ходе собеседований; за практические умения и навыки — оценка за ДЗ, ИЗ и КЗ; за добросовестность (оценка учитывает пропуски занятий без уважительных причин, качество подготовки к собеседованию и оформления ответа, своевременность сдачи и т.д.)

Итак, к каждому коллоквиуму нужно: а) ЗАРАНЕЕ ознакомиться с вопросами и подготовить ответы на них; б) подготовиться к защите ДЗ, ИЗ и КЗ; в) подготовиться к теоретическому собеседованию, проработав планы ответов, заучив важнейшие понятия, формулы и т.д.

Коллоквиум сдан, если по каждому вопросу предъявлен план ответа (дайджест), оформлены и защищены ДЗ, ИЗ и КЗ, пройдено теоретическое собеседование и показаны практические умения.

5. ПОРЯДОК СДАЧИ ЗАЧЕТА (ЭКЗАМЕНА)

Зачет (экзамен) включает 2 части: собеседование по теоретическому материалу; проверку практических умений и навыков. Вначале у каждого студента проверяется наличие планов ответов и записей ко второй части. При их отсутствии студент может быть не допущен к зачету (экзамену). Проверяется также, соответствуют ли планы ответов по сжатости предлагаемым ниже дайджестам: тексты ответов, конспекты лекций, учебники и т.п. запрещены, а всё, что требовалось заучить, должно быть в памяти, а не на бумаге.

Если у студента не выполнены какие-то домашние работы, имеются задолженности по практическим (лабораторным) занятиям, не сданы контрольные работы — ОН НЕ ВЫПОЛНИЛ УЧЕБНЫЙ ПЛАН И К ЗАЧЕТУ (ЭКЗАМЕНУ) НЕ ДОПУСКАЕТСЯ. Если задолженность невелика (не сдан 1 список понятий, не показано 1 домашнее задание и пр.), то можно договориться ликвидировать её на консультации перед зачетом (экзаменом) или даже в начале зачета (экзамена), пока готовятся первые студенты. Но этого времени мало...

Затем студент получает билет или номер соответствующих теоретического вопроса и практической задачи и готовится БЕЗ ИСПОЛЬЗОВАНИЯ планов ответа, записей.

На зачете (экзамене) проверяются: полнота раскрытия теоретического вопроса и свобода владения основными математическими понятиями; качество подготовки вопросов для самостоятельного изучения; качество владения практическими умениями и навыками. Зачет (экзамен) не сдан, если любая из трех оценок неудовлетворительна. Кроме того, итоговая оценка в зачетке учитывает оценки по итогам работы в семестре: за теоретические собеседования; за работу на лекциях; за решение задач. ВНИМАНИЕ! Второй билет даваться, как правило, не будет.