**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_2025_625.plx
02.03.01 Математика и компьютерные науки
Цифровые технологии

Квалификация **бакалавр**

Форма обучения **очная**

Общая трудоемкость **3 ЗЕТ**

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

Виды контроля в семестрах:
зачеты 6

**Распределение часов дисциплины по семестрам**

| Семестр (<Курс>.<Семестр на курсе>) | **6 (3.2)** | | Итого | |
|---|---|---|---|---|
| Недель | 15 5/6 | | | |
| Вид занятий | 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 30.01.2025 протокол № 2.

Рабочая программа утверждена на заседании кафедры
**кафедра математики, физики и информатики**

Протокол от 10.04.2025 протокол № 10

Зав. кафедрой Богданова Рада Александровна

**Визирование РПД для исполнения в очередном учебном году**

Рабочая программа пересмотрена, обсуждена и одобрена для исполнения в 2026-2027 учебном году на заседании кафедры
**кафедра математики, физики и информатики**

Протокол от __ _____ 2026 г. № __
Зав. кафедрой Богданова Рада Александровна

**Визирование РПД для исполнения в очередном учебном году**

Рабочая программа пересмотрена, обсуждена и одобрена для исполнения в 2027-2028 учебном году на заседании кафедры
**кафедра математики, физики и информатики**

Протокол от __ _____ 2027 г. № __
Зав. кафедрой Богданова Рада Александровна

**Визирование РПД для исполнения в очередном учебном году**

Рабочая программа пересмотрена, обсуждена и одобрена для исполнения в 2028-2029 учебном году на заседании кафедры
**кафедра математики, физики и информатики**

Протокол от __ _____ 2028 г. № __
Зав. кафедрой Богданова Рада Александровна

**Визирование РПД для исполнения в очередном учебном году**

Рабочая программа пересмотрена, обсуждена и одобрена для исполнения в 2029-2030 учебном году на заседании кафедры
**кафедра математики, физики и информатики**

Протокол от __ _____ 2029 г. № __
Зав. кафедрой Богданова Рада Александровна

| 1. ЦЕЛИ И ЗАДАЧИ ОСВОЕНИЯ ДИСЦИПЛИНЫ | |
|---|---|
| 1.1 | *Цели:* 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 | *Задачи:* 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: | Б1.О.16 |
| **2.1** | **Требования к предварительной подготовке обучающегося:** |
| 2.1.1 | Математический анализ |
| 2.1.2 | Алгебра |
| 2.1.3 | Теория чисел |
| 2.1.4 | Информационная безопасность |
| **2.2** | **Дисциплины и практики, для которых освоение данной дисциплины (модуля) необходимо как предшествующее:** |
| 2.2.1 | Выполнение 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** |
| знает основные задачи и понятия криптографии; |
| **ИД-2.ОПК-1: Умеет доказывать утверждения, решать задачи в области математических наук** |
| умеет 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** |
| владеет 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** |
| знает 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** |
| умеет 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** |
| владеет навыками использования типовых криптографических алгоритмов; |

| 4. СТРУКТУРА И СОДЕРЖАНИЕ ДИСЦИПЛИНЫ (МОДУЛЯ) | | | | | | | |
|---|---|---|---|---|---|---|---|
| **Код занятия** | **Наименование разделов и тем /вид занятия/** | **Семестр / Курс** | **Часов** | **Компетенции** | **Литература** | **Интеракт.** | **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 | 0 | |
| 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 | 0 | тест, коллоквиум, разноуровневые задачи, вопросы к зачету |
| 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 | доклад/сообщение |
| | **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 | 0 | |
| 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 | 0 | |
| 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-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-3.ОПК-4 | Л1.1 Л1.2Л2.1 | 0 | |
| 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-3.ОПК-4 | Л1.1 Л1.2Л2.1 | 0 | тест, коллоквиум, разноуровневые задачи, вопросы к зачету |
| 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-3.ОПК-4 | Л1.1 Л1.2Л2.1 | 0 | тест, коллоквиум, разноуровневые задачи, вопросы к зачету |
| 2.8 | Блочные шифры. ГОСТ 28147-89, IDEA и DES. Многочлены над Z2 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-3.ОПК-4 | Л1.1 Л1.2Л2.1 | 0 | тест, коллоквиум, разноуровневые задачи, вопросы к зачету |
| 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-3.ОПК-4 | Л1.1 Л1.2Л2.1 | 0 | тест, коллоквиум, разноуровневые задачи, вопросы к зачету |
| 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-3.ОПК-4 | Л1.1 Л1.2Л2.1 | 0 | тест, коллоквиум, разноуровневые задачи, вопросы к зачету |

| | | | | | | | |
|---|---|---|---|---|---|---|---|
| 2.11 | Вычисления в Zn. Шифр с открытым ключом: RSA, Эль-Гамаля, Шамира, Диффи-Хэллмана, Рабина, Гольдвассер -Микали, Блюма-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 | тест, коллоквиум, разноуровневые задачи, вопросы к зачету |
| 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 | доклад/сообщение |
| 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 | доклад/сообщение |
| 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 | доклад/сообщение |
| 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 | доклад/сообщение |
| 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 | доклад/сообщение |
| | **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 | 0 | |

| | | | | | | | |
|---|---|---|---|---|---|---|---|
| 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-3.ОПК-4 | Л1.1 Л1.2Л2.1 | 0 | |
| 3.3 | Реализация схемы ЭЦП: RSA, Эль-Гамаля и ее варианты, Фиата-Шамира, Онга-Шнорра-Шамира, Шнорра. Неотрицаемая подпись Шаума-ван-Антверпена. Эллиптические кривые над конечным полем. Преобразование криптосистемы над Zp 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-3.ОПК-4 | Л1.1 Л1.2Л2.1 | 0 | тест, коллоквиум, разноуровневые задачи, вопросы к зачету |
| 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-3.ОПК-4 | Л1.1 Л1.2Л2.1 | 0 | доклад/сообщение |
| 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-3.ОПК-4 | Л1.1 Л1.2Л2.1 | 0 | доклад/сообщение |
| | **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-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-3.ОПК-4 | Л1.1 Л1.2Л2.1 | 0 | тест, коллоквиум, разноуровневые задачи, вопросы к зачету |
| 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-3.ОПК-4 | Л1.1 Л1.2Л2.1 | 0 | доклад/сообщение |
| | **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 /КСРАтт/ | 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. Пояснительная записка

1. Назначение фонда оценочных средств. Оценочные средства предназначены для контроля и оценки образовательных достижений обучающихся, освоивших программу учебной дисциплины «Математические основы криптографии».
2. Фонд оценочных средств включает контрольные материалы для проведения текущего контроля в форме коллоквиума, тестовых заданий, разноуровневых заданий, тем для сообщений, докладов и вопросов к зачету.

### 5.2. Оценочные средства для текущего контроля

Примерный тест для входного контроля

1. Информационная безопасность характеризует защищенность:
А) Пользователя и информационной системы
Б) Информации и поддерживающей ее инфраструктуры
В) Источника информации
Г) Носителя информации

2. Что из перечисленного является составляющей информационной безопасности?
А) Нарушение целостности информации
Б) Проверка прав доступа к информации
В) Доступность информации
Г) Выявление нарушителей

3. Получение требуемой информации информационной услуги пользователем за определенное время, это:
А) Целостность информации
Б) Конфиденциальность информации
В) Доступность информации
Г) Защищенность информации

4. Конфиденциальность информации гарантирует:
А) Доступность информации кругу лиц, для кого она предназначена
Б) Защищенность информации от потери
В) Защищенность информации от фальсификации
Г) Доступность информации только автору

5. Сколько уровней формирования режима информационной безопасности?
А) Три

Б) Четыре
В) Два
Г) Пять

6.Год издания закона Российской Федерации «О государственной тайне»:
А) 2000 год
Б) 1993 год
В) 1995 год
Г) 1996 год

7. Номер статьи Уголовного кодекса предусматривающей наказание за разглашение государственной тайны?
А) 138
Б) 283
В) 273
Г) 237

8. Неправомерный доступ к компьютерной информации наказывается лишением свободы
А) До пяти лет
Б) До трех лет
В) До года
Г) До двух лет

9. Основной источник внутренних отказов?
А) Невозможность пользователя работать с системой в силу отсутствия соответствующей подготовки
Б) Нежелание пользователя работать с информационной системой
В) Отступление от установленных правил эксплуатации
Г) Нарушение работы систем связи, электропитания, водо- и/или теплоснабжения, кондиционирования

10. Уровни, не относящиеся к уровням формирования режима информационной безопасности?
А) Законодательно-правовой
Б) Информационный
В) Административный (организационный)
Г) Программно-технический

11. На сколько классов подразделяют угрозы информационной безопасности?
А) 4
Б) 3
В) 2
Г) 5

12. Что является самым эффективным при борьбе с непреднамеренными случайными ошибками?
А) Резервирование аппаратуры
Б) Определение степени ответственности за ошибки
В) Максимальная автоматизация и строгий контроль
Г) Контроль действий пользователя

13. Средства защиты информации какого из уровней формирования режима информационной безопасности связаны непосредственно с защищаемой информацией
А) Законодательно-правовой
Б) Информационный
В) Административный (организационный)
Г) Программно-технический

14. Основополагающим документом по информационной безопасности в РФ является:
А) Конституция РФ
Б) Уголовный кодекс
В) Закон о средствах массовой информации
Г) Закон об информационной безопасности

15. Целостность информации гарантирует:
А) Существование информации в исходном виде
Б) Принадлежность информации автору
В) Доступ информации определенному кругу пользователей
Г) Защищенность информации от несанкционированного доступа

16. Сколько категорий государственных информационных ресурсов определяет закон «Об информации, информатизации и защите информации»?
А) Три

Б) Четыре
В) Два
Г) Пять

17. Неправомерный доступ к компьютерной информации наказывается штрафом:
А) От 5 до 20 минимальных размеров оплаты труда
Б) От 200 до 500 минимальных размеров оплаты труда
В) От 150 до 200 минимальных размеров оплаты труда
Г) До 300 минимальных размеров оплаты труда

18. Нарушение правил эксплуатации ЭВМ, системы ЭВМ или их сети наказывается ограничением свободы на срок:
А) До года
Б) До двух лет
В) До пяти лет
Г) До трех месяцев

19. Защищенность информации и поддерживающей ее инфраструктуры от случайных или преднамеренных воздействий естественного или искусственного характера, которые могут нанести ущерб владельцам или пользователям информации — это:
А) Компьютерная безопасность
Б) Информационная безопасность
В) Защита информации
Г) Защита государственной тайны

20. Что из перечисленного является задачей информационной безопасности?
А) Устранение неисправностей аппаратных средств
Б) Устранение последствий стихийных бедствий
В) Защита технических и программных средств информатизации от ошибочных действий персонала
Г) Восстановление линий связи

21. Выберите правильную иерархию пространства требований в «Общих критериях»:
А) Класс — семейство — компонент — элемент
Б) Элемент — класс — семейство — компонент
В) Компонент — семейство — класс — элемент
Г) Семейство — компонент — класс — элемент

22. Сколько классов СВТ по уровню защищенности от НСД к информации определено в руководящем документе Гостехкомиссии «СВТ. Защита от НСД к информации. Показатели защищенности от НСД к информации»?
А) Три
Б) Семь
В) Пять
Г) Четыре
23. Комплекс предупредительных мер по обеспечению информационной безопасности организации — это:
А) Информационная политика
Б) Политика безопасности
В) Информационная безопасность
Г) Защита информации

24. Аутентичность связана:
А) С доказательством авторства документа
Б) С проверкой прав доступа
В) С изменением авторства документа
Г) С контролем целостности данных

25. Что не рассматривается в политике безопасности?
А) Требуемый уровень защиты данных
Б) Роли субъектов информационных отношений
В) Анализ рисков
Г) Защищенность механизмов безопасности

Примерный тест для текущего контроля №1

1. Что такое криптография?
а) отрасль знаний, целью которой является изучение и создание криптографических преобразований и алгоритмов;
б) Совокупность методов взлома информации;
в) Совокупность средств генерации ПСЧ.

2. К какому классу преобразований относится шифр Цезаря?
а) является вариацией метода гаммирования;
б) это хэш функция;
в) шифр Цезаря представляет собой простой подстановочный фильтр.

3. Шифр подстановки - это ...
а) это вариация асимметричной криптосистемы;
б) шифр, работающий на основе аппарата необратимых функций;
в) Подстановочным шифром называется шифр, который каждый символ открытого текста в шифротексте заменяет другим символом. Получатель инвертирует подстановку шифротекста, восстанавливая открытый текст.

4. Какие из перечисленных ниже алгоритмов не являются симметричными?
а) Все нижеперечисленные;
б) Шифры гаммирования;
г) шифры подстановки (Цезарь, Вижнер, Вернам, и т.п.);
д) шифры перестановки (Квадрат Полибия, Квадрат Кардано, поворотные решетки)
е) RSA;
ж) алгоритмы на эллиптических кривых;
и) FAPKC1;
к) Data Encription Standart.

5. Какую длину имеет секретный ключ в криптосистеме DES?
а) разрядность блока - 32бита, размер ключа - 32бит;
б) разрядность блока - 64 бита, размер ключа - 56 бит (с учетом контрольных разрядов - 64 бита);
в) разрядность блока - 64 бита, размер ключа - 128 бит (с учетом контрольных разрядов - 96 бита).

6. Какая архитектура лежит в основе алгоритма DES?
а) Алгоритм представляет собой классическую сеть Файстеля из нескольких раундов с добавлением входной и выходной перестановки бит;
б) Алгоритм представляет автомат Мили;
в) Алгоритм представляет автомат Мура.

7. Блочные криптоалгоритмы используют размер блока...
а) Произвольный;
б) Строго определенный, равный 64, 128 или 256 битам;
в) Строго определенный, равный 130, 230 или 330 битам.

8. Что такое раунд (round)?
а) один шаг шифрования в шифре Файстеля и близких ему по архитектуре шифрах, в ходе которого одна или несколько частей шифруемого блока данных подвергается модификации;
б) окружность;
в) частный случай эллиптической кривой.

9. Какая процедура распределения ключей не требует использования защищенного канала для передачи секретного ключа адресату?
а) Метод Диффи – Хеллмана;
б) Метод гаммирования;
в) Метод хэш-функций.

10. Какая процедура является более производительной по сравнению с другой?
а) асимметричное шифрование/дешифрование;
б) симметричное шифрование/дешифрование;
в) варианты а) и б) обладают одинаковой производительностью.

11. Какая из ниже приведенных систем с открытым ключом используется исключительно для генерации цифровой подписи?
а) DES;
б) система Вернама;
в) Digital Signature Algorithm (DSA).

12. Какой шифр из ниже перечисленных шифров является абсолютно стойким шифром?
а) DES;
б) система Вернама;
в) Digital Signature Algorithm (DSA).

13. Какие трудноразрешимые задачи используются для повышения стойкости алгоритма RSA?
а) трудоемкости разложения на множители больших чисел;
б) трудоемкость задачи останова на машине Тьюринга;

в) трудоемкость задачи коммивояжера.

14. Что такое односторонняя хэш-функция?
а) функция, являющаяся вычислительно необратимой функцией;
б) частный случай функций, заданных таблично;
в) функция, реализующая автоматные схемы.

15. Какой объем информации отводится под результат вычисления хэш-функции по алгоритму SHA-1?
а) 64 бита;
б) 128 бит;
в) 160 бит.

Примерный тест для текущего контроля №2

1. Проблема дискретного логарифма заключается ...
а) зная основание степени и получившийся после возведения результат по модулю простого числа, невозможно за обозримое время определить, в какую именно степень было возведено основание;
б) невозможно реализовать эффективный алгоритм его вычисления;
в) не никаких вычислительных проблем.

2. Какие алгоритмы не используются для вычисления дайджеста сообщения?
а) схема Вижинера;
б) MD4;
в) DES.

3. Когда необходимо ввести в состав оборудования организации межсетевой экран?
а) когда требуется повысить скорость обмена данными с внешними сетями;
б) когда необходимо моделировать и исследовать активность хакеров;
в) при внедрении политики компьютерной безопасности.

4. Какие задачи выполняют VPN?
а) обеспечение удаленного защищенного доступа через открытые Интернет-каналы к серверам баз данных, Web-, FTP- и почтовым серверам;
б) это подход к разработке асинхронных алгоритмов шифрования;
в) это подход к разработке синхронных алгоритмов шифрования.

5. Какой протокол был разработан для обеспечения системы электронных банковских расчетов с использованием пластиковых карт?
а) Secure Key Internet Protocol;
б) Secure Electronic Transactions;
в) Secure sockets layer.

6. Дешифрование - это ...
а) Получение открытых данных по зашифрованным в условиях, когда алгоритм расшифрования не является полностью (вместе со всеми секретными параметрами) известным и расшифрование не может быть выполнено обычным путем;
б) процесс обратный процессу шифрования, т. е. восстановление с помощью соответствующего ключа информации в исходной форме, позволяющей извлечь из нее смысловые данные;
в) вычисление хэш-функции зашифрованного сообщения.

7. Криптоанализ - это...
а) Отрасль, занимающаяся исследованием эффективности методов шифрования сообщений;
б) Отрасль знаний, целью которой является поиск и исследование методов взлома криптографических алгоритмов, а также сама процедура взлома;
в) Отрасль, связанная с разработкой электронных подписей.

8. К какому классу преобразований относится система шифрования Вижинера?
а) Блочный шифр;
б) Шифр на основе автоматов;
в) Многоалфавитный подстановочный шифр.

9. Какие секретные ключи поддерживает алгоритм Rijdael?
а) Длина ключа является изменяемой;
б) Длина ключа кратна 32;
в) Нет никаких ограничений, накладываемых на ключи.

10. Что такое “сеть Файстеля” (Feistel network)?

а) архитектура построения блочных шифров, в которой весь процесс шифрования блока выполняется за серию шагов (раундов), на каждом из которых блок делится на изменяемую и постоянную части;
б) архитектура построения шифров на основе автомата Мили;
в) архитектура генератора псевдослучайных чисел.

11. Какое свойство присуще асимметричной системе.
а) transaction (транзакционность);
б) dependency injection (внедрение зависимости);
в) trapdoor (потайная дверь).

12. Какие из ниже приведенных систем с открытым ключом используются для шифрования информации?
а) DES, ГОСТ 28147-89;
б) RSA, схема Рабина (развитие - схема Вильямса);
в) Схема Вернама;
г) Алгоритм Евклида.

13. Какая трудноразрешимая задача в основе алгоритма обмена ключами Диффи-Хэллмана?
а) Задача дискретного логарифмирования;
б) Задача коммивояжера;
в) Задача полного перебора.

14. Что такое SP-сеть?
а) Разновидность асимметричной системы;
б) Разновидность блочного шифра;
в) Разновидность клеточного автомата.

15. Доказательство с нулевым разглашением должно обладать свойствами (выберите несколько из предложенных):
а) Полнота;
б) Корректность;
в) Доступность;
г) Целостность;
д) Нулевое разглашение.

Критерии оценки:
- Оценка «отлично» выставляется студенту, если он дал правильные ответы в диапазоне 85-100%, тем самым показав знание математических основ криптографии, умение применять эти знания.
- Оценка «хорошо» выставляется студенту, если он дал правильные ответы на 76-84% вопросов теста, тем самым показав неплохое знание математических основ криптографии, умение применять эти знания.
- Оценка «удовлетворительно» выставляется студенту, если он дал правильные ответы на 61-75% вопросов, показав посредственное знание математических основ криптографии, несистемное умение применять эти знания.
- Оценка «неудовлетворительно» выставляется студенту, если он дал правильные ответы менее чем на 61% вопросов, показав знание только отдельных положений математических основ криптографии, слабое умение применять эти фрагментарные знания.

Комплект разноуровневых задач/заданий

Задачи репродуктивного уровня
1. Разработать алгоритм шифрования с использованием шифров замены.
2. Разработать алгоритм шифрования с использованием шифра перестановки.
3. Разработать алгоритм шифрования с использованием квадрата Полибия.
4. Разработать алгоритм шифрования с использованием метода прямой замены.
5. Разработать алгоритм шифрования с использованием алгоритма моноалфавитной замены.
6. Разработать алгоритм шифрования с использованием методов полиалфавитной замены.
7. Разработать алгоритм шифрования с использованием (матрицы) Виженера.
8. Разработать алгоритм шифрования с использованием методов перестановки.
9. Разработать алгоритм шифрования с использованием маршрутов Гамильтона.
10. Разработать алгоритм шифрования с использованием аналитических методов шифрования.
11. Разработать алгоритм шифрования с использованием методов шифрования, основанных на использовании матричной алгебры.
12. Разработать алгоритм шифрования с использованием аддитивных методов шифрования.
13. Разработать алгоритм шифрования с использованием аддитивных методов, в основу которых положено использование генераторов (датчиков) псевдослучайных чисел.
14. Разработать алгоритм шифрования с использованием системы шифрования с открытым ключом.
15. Разработать алгоритм шифрования с использованием RSA.

Задачи реконструктивного уровня
1. Число является произведением двух простых чисел p и q, причем $|p-q|<500$. Разложить это число на простые

множители.
2. Сколько имеется натуральных чисел, меньших N=pq и взаимно простых с N, где p и q — различные простые числа?
3. Известно, что число N=203060593 является произведением двух простых чисел p и q, а количество натуральных чисел, меньших и взаимно простых с N, равно 203030388. Найдите числа p и q.
4. Пусть N=713 является произведением двух простых чисел p и q. Найти эти числа.
5. Для открытия подземелья в волшебной стране надо правильно назвать три целых числа a, b, c, служащих коэффициентами квадратичной функции f(x) = ax^2 + bx + c . Представителям четырёх рас были переданы следующие значения функции: троллям — значение f(21), эльфам — f(24) , гномам — f(25) , оркам — f(28) . Когда представители рас встретились, чтобы совместно найти a, b, c и открыть подземелье, один из представителей, чтобы сорвать мероприятие, предъявил неверное значение. Выясните, кто это был, если известно, что тролли предъявили число 273, эльфы — 357, гномы — 391, орки — 497.

Задачи творческого уровня
1. Как преобразовать протокол аутентификации запрос-ответ на базе схемы открытого шифрования в протокол аутентичного распределения ключей? Приведите два примера: для протокола односторонней аутентификации и для протокола взаимной аутентификации.
2. Приведите описание процедуры восстановления секрета из схемы разделения секрета Шамира двумя способами: для случая, когда общее число участников равно 3, максимально допустимое количество утраченных (скомпроментированных) долей секрета равно 2, длина разделяемого секрета равно 128 битам.
3. Какими из основных свойств протоколов распределения ключей (неявная аутентификация ключа, подтверждение ключа, явная аутентификация) обладает протокол Kerberos? Какие практические задачи он позволяет решать?
4. Оцените вычислительную сложность (количество выполненных операций) и коммуникационную сложность (количество пересылок сообщений и объем передаваемых данных) протокола доказательства знания дискретного логарифма для каждого участника. Приведите пример такого задания параметров протокола, при котором вероятность обмана доказывающим проверяющего не превысит 2^(-30).
5. Сравните по стойкости к различным видам атак два метода аутентификации по одноразовым паролям: метод Лэмпорта и последовательно обновляемые одноразовые пароли. Какие выводы о предпочтительности того или иного метода можно сделать?

Критерии оценки:
«Отлично», повышенный уровень: выполнены задания репродуктивного, реконструктивного и творческого уровня.
«Хорошо», пороговый уровень: выполнены задания репродуктивного, реконструктивного и некоторые задания творческого уровня.
«Удовлетворительно», пороговый уровень: выполнены задания лишь репродуктивного и реконструктивного уровня.
«Неудовлетворительно», уровень не сформирован: выполнены задания репродуктивного уровня или задания вовсе не выполнены.

Вопросы к коллоквиуму

1. Перечислите и кратко охарактеризуйте основные задачи обеспечения информационной безопасности, решаемые с помощью криптографических методов.
2. Раскройте определения: шифрование, зашифрование, расшифрование, дешифрование.
3. Чем шифрование отличается от кодирования?
4. Приведите известные вам классификации криптосистем.
5. Укажите основные отличия между современной и классической криптографией.
6. Сравните аффинный шифр и шифр Хилла с точки зрения криптостойкости.
7. Опишите способы криптоанализа.
8. Сравните криптосистему RSA и криптосистему Эль-Гамаля.
9. Укажите основной недостаток кодов аутентичности сообщений.
10. Дайте понятие криптографического протокола.
11. Укажите основные отличия между современными и классическими блочными шифрами.
12. Перечислите режимы работы ГОСТ 28147-89. Для чего служит каждый из данных режимов?
13. Сравните DES и ГОСТ 28147-89.
14. Сравните AES и ГОСТ 28147-89.
15. Перечислите основные свойства хеш-функций.
16. Чем хеширование отличается от выработки контрольных сумм?
17. Чем хеширование отличается от выработки имитовставки?
18. Укажите два подхода к построению функций хеширования.

Критерии оценки:
«Отлично», повышенный уровень: изложение полученных знаний в устной, письменной или графической форме, полное, в системе, в соответствии с требованиями учебной программы; допускаются единичные несущественные ошибки, самостоятельно исправляемые студентами;
«Хорошо», пороговый уровень: изложение полученных знаний в устной, письменной и графической форме, полное, в системе, в соответствии с требованиями учебной программы; допускаются отдельные несущественные ошибки,

исправляемые студентами после указания преподавателя на них;
«Удовлетворительно», пороговый уровень: изложение полученных знаний неполное, однако это не препятствует усвоению последующего программного материала; допускаются отдельные существенные ошибки, исправленные с помощью преподавателя;
«Неудовлетворительно», уровень не сформирован: изложение учебного материала неполное, бессистемное, что препятствует усвоению последующей учебной информации; существенные ошибки, неисправляемые даже с помощью преподавателя.

**5.3. Темы письменных работ (эссе, рефераты, курсовые работы и др.)**

Темы сообщений и докладов

1. Обзор методов криптоанализа по сторонним каналам.
2. Алгебраический криптоанализ шифров: перспективы.
3. Максимально-нелинейные булевы функции: открытые проблемы.
4. Криптоанализ шифра AES. Обзор результатов.
5. Обзор докладов конференции Boolean Functions and Applications (BFA) текущего года.
6. Современные методы стеганографии.
7. Обзор развития способов проектирования блочных шифров
8. Криптография в программных продуктах: PGP, Skype, WhatsApp, Zoom и др.
9. Дифференциальный (разностный) криптоанализ и его применение на практике.
10. Современные способы обеспечения информационной безопасности.
11. Постквантовая криптография: обзор криптосистем, основанных на кодах, исправляющих ошибки.
12. Технология блокчейн и распределенные реестры: современное состояние.
13. Квантовый криптоанализ и квантовая криптография: перспективы, последние результаты.
14. Конкурсы криптографических стандартов: NIST Post Quantum.

Критерии оценки:
«Отлично», повышенный уровень: системность, обстоятельность и глубина излагаемого материала; знакомство с научной и научно-популярной литературой, рекомендованной к докладу преподавателем; письменная форма доклада (от руки); способность воспроизвести основные тезисы доклада без помощи конспекта; способность быстро и развернуто отвечать на вопросы преподавателя и аудитории; способность докладчика привлечь внимание аудитории.
«Хорошо», пороговый уровень: развернутость и глубина излагаемого в докладе материала; знакомство с основной научной литературой к докладу; письменная форма доклада; при выступлении частое обращение к тексту доклада; некоторые затруднения при ответе на вопросы (неспособность ответить на ряд вопросов из аудитории).
«Удовлетворительно», пороговый уровень: правильность основных положений доклада; наличие недостатка информации в докладе по целому ряду проблем; использование для подготовки доклада исключительно учебной литературы; неспособность ответить на несложные вопросы из аудитории и преподавателя; неумение воспроизвести основные положения доклада без письменного конспекта.
«Неудовлетворительно», уровень не сформирован: подготовка доклада в печатном виде с привлечением неизвестного информационного источника; поверхностный, неупорядоченный, бессистемный характер информации в докладе; при чтении доклада постоянное использование текста; выступление сбивчивое, с долгими паузами, монотонное; полное отсутствие внимания к докладу аудитории.

**5.4. Оценочные средства для промежуточной аттестации**

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 нетексто¬вых 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-Гамаля. 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-Гамаля.
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 Zp к шифру (ЭЦП) на эллиптической кривой.
53. Шифр Эль-Гамаля на эллиптической кривой.
54. Стандарты ЭЦП на эллиптической кривой: ГОСТ Р 34.10-2001, ECDSA.

Критерии итоговой оценки по дисциплине (зачет)

«Зачтено», повышенный уровень: теоретическое содержание дисциплины освоено полностью, без пробелов, необходимые практические навыки работы с освоенным материалом сформированы, все предусмотренные рабочей программой дисциплины учебные задания выполнены, качество их выполнения оценено числом баллов, близким к максимальному;
«Зачтено», пороговый уровень: теоретическое содержание дисциплины освоено частично, но пробелы не носят существенного характера, необходимые практические навыки работы с освоенным материалом в основном сформированы, большинство предусмотренных рабочей программой дисциплины учебных заданий выполнено, некоторые из выполненных заданий, возможно, содержат ошибки;
«Не зачтено», уровень не сформирован: теоретическое содержание дисциплины не освоено. Необходимые практические навыки работы не сформированы, все предусмотренные рабочей программой дисциплины учебные задания выполнены с грубыми ошибками. Дополнительная самостоятельная работа над материалом дисциплины не приведет к какому-либо значимому повышению качества выполнения учебных заданий.

Контрольные тесты и задания

Название вопроса: 1 (ОПК-1)
Формулировка вопроса: Криптография изучает:
Варианты ответов: 1) построение и использование систем шифрования, в том числе их стойкость, слабости и степень уязвимости относительно различных методов вскрытия; 2) методы расшифровки зашифрованной информации без предназначенного для такой расшифровки ключа и сам процесс такой расшифровки; 3) методы шифрования и дешифрования; 4) методы скрытой передачи информации путём сохранения в тайне самого факта передачи
Ключ: 1) построение и использование систем шифрования, в том числе их стойкость, слабости и степень уязвимости относительно различных методов вскрытия.

Название вопроса: 2 (ОПК-4)
Формулировка вопроса: Какая алгебраическая структура из приведенного списка является абелевой группой?
Варианты ответов: 1) Множество целых чисел относительно операции умножения; 2) Множество целых чисел относительно операции сложения; 3) Множество натуральных чисел относительно операции умножения; 4) Множество действительных чисел относительно операции извлечения квадратного корня
Ключ: 2) Множество целых чисел относительно операции сложения.

Название вопроса: 3 (ОПК-1)
Формулировка вопроса: В кольце могут быть делители нуля.
Ключ: Верно.

Название вопроса: 4 (ОПК-4)
Формулировка вопроса: Шифр гаммирования устойчив к атакам методом частотного анализа.
Ключ: Верно.

Название вопроса: 5 (ОПК-1)
Формулировка вопроса: Найдите обратный класс к 16-му классу в кольце классов вычетов по модулю 33. В ответе укажите наименьший неотрицательный вычет из получившегося класса.
Ключ: 31.

Название вопроса: 6 (ОПК-4)
Формулировка вопроса: Сколько простых делителей содержит число 2627?
Ключ: 2.

Название вопроса: 7 (ОПК-1)
Формулировка вопроса: Выберите верные соответствия
Ключ:
Значение:
Верный ответ:
Шифр устойчив к атакам методом частотного анализа
Шифр Хилла
Шифр неустойчив к атакам методом частотного анализа
Аффинный шифр
Шифр является абсолютно стойким
Шифр Вернама
Шифр является простейшим примером шифра простой замены
Шифр Цезаря

Название вопроса: 8 (ОПК-4)
Формулировка вопроса: Выберите верные соответствия
Ключ:
Значение:
Верный ответ:
Ассоциативное коммутативное кольцо с единицей, отличной от нуля, без делителя нуля
Поле
Множество классов вычетов по заданному модулю относительно операций сложения и умножения
Коммутативно-ассоциативное кольцо с единицей
Множество квадратных матриц одинакового порядка с элементами из множества классов вычетов по заданному модулю относительно операций сложения и умножения Некоммутативное ассоциативное кольцо с единицей
Множество подстановок порядка n относительно операции композиции
Некоммутативная группа

## 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 университет, 2017 | http://www.iprbookshop.ru/75601.html |

| | Авторы, составители | Заглавие | Издательство, год | Эл. адрес |
|---|---|---|---|---|
| Л1.2 | Игнатьев Е. Б. | Основы криптографии: учебное пособие | Иваново: ИГЭУ, 2020 | https://e.lanbook.com/book/154559 |
| **6.1.2. Дополнительная литература** | | | | |
| | Авторы, составители | Заглавие | Издательство, год | Эл. адрес |
| Л2.1 | Пономарчук Ю. В. | Основы анализа шифров классической криптографии: учебное пособие | Хабаровск: ДВГУПС, 2019 | https://e.lanbook.com/book/179357 |

| **6.3.1 Перечень программного обеспечения** | |
|---|---|
| 6.3.1.1 | Adobe Reader |
| 6.3.1.2 | Яндекс.Браузер |
| 6.3.1.3 | Kaspersky Endpoint Security для бизнеса СТАНДАРТНЫЙ |
| 6.3.1.4 | MS Office |
| 6.3.1.5 | NVDA |
| 6.3.1.6 | LibreOffice |
| 6.3.1.7 | РЕД ОС |
| 6.3.1.8 | MS Windows |
| **6.3.2 Перечень информационных справочных систем** | |
| 6.3.2.1 | Межвузовская электронная библиотека |
| 6.3.2.2 | Электронно-библиотечная система «Издательство Лань» |
| 6.3.2.3 | База данных «Электронная библиотека Горно-Алтайского государственного университета» |
| 6.3.2.4 | Электронно-библиотечная система IPRbooks |

| **7. ОБРАЗОВАТЕЛЬНЫЕ ТЕХНОЛОГИИ** | | |
|---|---|---|
| | проблемная лекция | |
| | кластер | |
| | лекция с запланированными ошибками | |
| | круглый стол | |

| **8. МАТЕРИАЛЬНО-ТЕХНИЧЕСКОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ (МОДУЛЯ)** | | |
|---|---|---|
| **Номер аудитории** | **Назначение** | **Основное оснащение** |
| 207 Б1 | Лекционная аудитория. 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, проектор, экран, системный блок, посадочные места обучающихся (по количеству обучающихся), рабочее место преподавателя |
| 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 | Рабочее место преподавателя. Посадочные места обучающихся (по количеству обучающихся). Маркерная ученическая доска, экран, мультимедиапроектор, 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 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 прочитав 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 данная 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 символьные 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 пятерки 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 каково 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 учить 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 штурм 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 зачётке 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.