МИНОБРНАУКИ РОССИИ

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

Методы и средства защиты коммерческой информации

рабочая программа дисциплины (модуля)

Закреплена за кафедрой **кафедра экономики, туризма и прикладной информатики**

Учебный план 09.04.03_2022_892М.plx
09.04.03 Прикладная информатика
Цифровая экономика

Квалификация **магистр**

Форма обучения **очная**

Общая трудоемкость **3 ЗЕТ**

Часов по учебному плану 108
в том числе:
аудиторные занятия 34
самостоятельная работа 65
часов на контроль 8,85

Виды контроля в семестрах:
зачеты с оценкой 3

Распределение часов дисциплины по семестрам

Семестр (<Курс>.<Семестр на курсе>)	**3 (2.1)**		Итого	
Недель	17 2/6			
Вид занятий	УП	РП	УП	РП
Лабораторные	26	26	26	26
Практические	8	8	8	8
Контроль самостоятельной работы при проведении аттестации	0,15	0,15	0,15	0,15
Итого ауд.	34	34	34	34
Контактная работа	34,15	34,15	34,15	34,15
Сам. работа	65	65	65	65
Часы на контроль	8,85	8,85	8,85	8,85
Итого	108	108	108	108

Программу составил(и):
к.ф.-м.н., доцент, Губкина Елена Владимировна _____

Рабочая программа дисциплины
Методы и средства защиты коммерческой информации

разработана в соответствии с ФГОС:
Федеральный государственный образовательный стандарт высшего образования - магистратура по направлению подготовки 09.04.03 Прикладная информатика (приказ Минобрнауки России от 19.09.2017 г. № 916)

составлена на основании учебного плана:
09.04.03 Прикладная информатика
утвержденного учёным советом вуза от 17.06.2022 протокол № 6.

Рабочая программа утверждена на заседании кафедры
кафедра экономики, туризма и прикладной информатики

Протокол от 17.06.2022 протокол № 11/1

Зав. кафедрой Куттубаева Тосканай Айтмукановна

Визирование РПД для исполнения в очередном учебном году

Рабочая программа пересмотрена, обсуждена и одобрена для исполнения в 2023-2024 учебном году на заседании кафедры
кафедра экономики, туризма и прикладной информатики

Протокол от __ _____ 2023 г. № __
Зав. кафедрой Куттубаева Тосканай Айтмукановна

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 экономики, туризма и прикладной информатики

Протокол от __ _____ 2024 г. № __
Зав. кафедрой Куттубаева Тосканай Айтмукановна

Визирование РПД для исполнения в очередном учебном году

Рабочая программа пересмотрена, обсуждена и одобрена для исполнения в 2025-2026 учебном году на заседании кафедры
кафедра экономики, туризма и прикладной информатики

Протокол от __ _____ 2025 г. № __
Зав. кафедрой Куттубаева Тосканай Айтмукановна

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 экономики, туризма и прикладной информатики

Протокол от __ _____ 2026 г. № __
Зав. кафедрой Куттубаева Тосканай Айтмукановна

1. ЦЕЛИ И ЗАДАЧИ ОСВОЕНИЯ ДИСЦИПЛИНЫ	
1.1	*Цели:* сформировать у студентов магистратуры системные знания о проблемах защиты информации и управления информационными рисками, организации защиты коммерческой тайны на предприятии, обеспечении ее безопасности, а также актуальных вопросах безопасности предпринимательских структур.
1.2	*Задачи:* изучить принципы защиты информации, организационные и административные методы защиты информации, программно-аппаратные средства защиты компьютерных систем, заложить основы системного подхода к организации защиты информации, передаваемой и обрабатываемой техническими средствами, на основе применения криптографических методов; изучить математические основы построения криптографических алгоритмов, правовые механизмы защиты коммерческой информации, методологию и методы защиты результатов своего интеллектуального труда, в том числе в форме коммерческой тайны и научиться применять их на практике; провести обзор готовых решений по обеспечению комплексной информационной безопасности на предприятии.

2. МЕСТО ДИСЦИПЛИНЫ В СТРУКТУРЕ ООП	
Цикл (раздел) ООП:	Б1.В.04
2.1	**Требования к предварительной подготовке обучающегося:**
2.1.1	Менеджмент в профессиональной деятельности
2.2	**Дисциплины и практики, для которых освоение данной дисциплины (модуля) необходимо как предшествующее:**
2.2.1	Выполнение и защита выпускной квалификационной работы
2.2.2	Технологическая (проектно-технологическая) практика

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

ПК-5: Способен использовать передовые методы оценки качества, надежности и информационной безопасности ИС в цифровой экономике

ИД-1.ПК-5: Определяет требования к качеству, надежности и информационной безопасности ИС в цифровой экономике

знать международные нормы в области оценки качества, надежности и информационной безопасности ИС, основные руководящие документы по реализации защиты информации, применительно к корпоративной ИС, основы проведения политики безопасности; уметь разрабатывать техническую документацию по вопросам обеспечения информационной безопасности ИС, анализировать показатели развития информационных технологий на предприятиях и в организациях, применять международные нормы в области оценки качества, надежности и информационной безопасности ИС; владеть навыками обоснования архитектуры ИС, оценки качества, надежности и информационной безопасности ИС в соответствии с международными стандартами;

ИД-2.ПК-5: Осуществляет выбор методов оценки качества, надежности и информационной безопасности ИС в цифровой экономике

знать основные угрозы информационной безопасности, методы, технологии и средства автоматизированного создания, адаптации, тестирования, испытаний и ввода ИС в действие, методы управления информационной безопасностью на предприятиях и в организациях, криптографические алгоритмы шифрования, российские стандарты для криптографической защиты информации, применительно к корпоративной ИС, основы хэш-функций, основы реализации электронной цифровой подписи; уметь оценивать качество, надежность и информационную безопасность ИС, давать оценку эффективности используемых методов и средств защиты компьютерной информации; владеть методами оценки качества, надежности и информационной безопасности ИС;

ИД-3.ПК-5: Использует передовые методы оценки качества, надежности и информационной безопасности ИС в цифровой экономике

знать методы оценки экономической эффективности внедряемой ИС, методы и средства защиты компьютерной информации на предприятиях и в организациях, технологии и средства автоматизированного создания и внедрения ИС в действие, программно-технические средства информационной безопасности; уметь выявлять, оценивать и прогнозировать источники угроз информационной безопасности, разрабатывать криптографические системы на основе российских стандартов; разрабатывать системы реализации электронной цифровой подписи; владеть методами анализа степени защиты корпоративной ИС, способами оптимизации ИТ-процессов, определения ресурсов, необходимых для обеспечения надежности функционирования ИС.

4. СТРУКТУРА И СОДЕРЖАНИЕ ДИСЦИПЛИНЫ (МОДУЛЯ)							
Код занятия	**Наименование разделов и тем /вид занятия/**	**Семестр / Курс**	**Часов**	**Компетен-ции**	**Литература**	**Инте ракт.**	**Примечание**
	Раздел 1. Методы и средства организационно-правовой защиты информации						
1.1	Информационные отношения и правовой режим защиты информации ограниченного доступа /Лаб/	3	1	ИД-1.ПК-5 ИД-2.ПК-5 ИД-3.ПК-5	Л1.1 Л1.2 Л1.3Л2.1 Л2.2	0	
1.2	Правовая защита различных видов конфиденциальной информации. /Лаб/	3	1	ИД-1.ПК-5 ИД-2.ПК-5 ИД-3.ПК-5	Л1.1 Л1.2 Л1.3Л2.1 Л2.2	0	
1.3	Защита персональных данных и государственное регулирование деятельности по защите информации /Лаб/	3	2	ИД-1.ПК-5 ИД-2.ПК-5 ИД-3.ПК-5	Л1.1 Л1.2 Л1.3Л2.1 Л2.2	0	
1.4	Основные понятия и организация защиты государственной и коммерческой тайны /Лаб/	3	2	ИД-1.ПК-5 ИД-2.ПК-5 ИД-3.ПК-5	Л1.1 Л1.2 Л1.3Л2.1 Л2.2	0	
1.5	Организация охраны, режима и работы с персоналом /Лаб/	3	2	ИД-1.ПК-5 ИД-2.ПК-5 ИД-3.ПК-5	Л1.1 Л1.2 Л1.3Л2.1 Л2.2	0	
1.6	Организация защиты информации в различных направлениях деятельности предприятия (организации) /Лаб/	3	2	ИД-1.ПК-5 ИД-2.ПК-5 ИД-3.ПК-5	Л1.1 Л1.2 Л1.3Л2.1 Л2.2	0	
1.7	Информационные отношения как объект правового регулирования. Законодательство Российской Федерации в области информационной безопасности /Пр/	3	1	ИД-1.ПК-5 ИД-2.ПК-5 ИД-3.ПК-5	Л1.1 Л1.2 Л1.3Л2.1 Л2.2	0	круглый стол
1.8	Институт правовой защиты коммерческой тайны /Пр/	3	1	ИД-1.ПК-5 ИД-2.ПК-5 ИД-3.ПК-5	Л1.1 Л1.2 Л1.3Л2.1 Л2.2	0	
1.9	Организация работы службы безопасности предприятия /Пр/	3	1	ИД-1.ПК-5 ИД-2.ПК-5 ИД-3.ПК-5	Л1.1 Л1.2 Л1.3Л2.1 Л2.2	0	
1.10	Комплексная защита государственной, служебной, коммерческой тайны и конфиденциальной информации /Ср/	3	3	ИД-1.ПК-5 ИД-2.ПК-5 ИД-3.ПК-5	Л1.1 Л1.2 Л1.3Л2.1 Л2.2	0	
1.11	Порядок отнесения сведений к коммерческой тайне предприятия, фирмы /Ср/	3	4	ИД-1.ПК-5 ИД-2.ПК-5 ИД-3.ПК-5	Л1.1 Л1.2 Л1.3Л2.1 Л2.2	0	
1.12	Методические основы экспертной оценки научно-технических и других сведений с грифом «Коммерческая тайна» («КТ») /Ср/	3	2	ИД-1.ПК-5 ИД-2.ПК-5 ИД-3.ПК-5	Л1.1 Л1.2 Л1.3Л2.1 Л2.2	0	
1.13	Участие правоохранительных органов и служб безопасности в защите коммерческой тайны /Ср/	3	4	ИД-1.ПК-5 ИД-2.ПК-5 ИД-3.ПК-5	Л1.1 Л1.2 Л1.3Л2.1 Л2.2	0	ситуационное задание
1.14	Инструкция по оформлению, учету, хранению и доступу к материалам с грифом «Коммерческая тайна» /Ср/	3	5	ИД-1.ПК-5 ИД-2.ПК-5 ИД-3.ПК-5	Л1.1 Л1.2 Л1.3Л2.1 Л2.2	0	
	Раздел 2. Методы и средства инженерно-технической и криптографической защиты информации						
2.1	Технические методы и средства защиты информации /Лаб/	3	2	ИД-1.ПК-5 ИД-2.ПК-5 ИД-3.ПК-5	Л1.1 Л1.2 Л1.3Л2.1 Л2.2	0	

2.2	Программно-аппаратные методы и средства защиты информации /Лаб/	3	2	ИД-1.ПК-5 ИД-2.ПК-5 ИД-3.ПК-5	Л1.1 Л1.2 Л1.3Л2.1 Л2.2	0	
2.3	Математические основы криптографии /Лаб/	3	2	ИД-1.ПК-5 ИД-2.ПК-5 ИД-3.ПК-5	Л1.1 Л1.2 Л1.3Л2.1 Л2.2	0	
2.4	Методы шифрования с закрытым ключом /Лаб/	3	2	ИД-1.ПК-5 ИД-2.ПК-5 ИД-3.ПК-5	Л1.1 Л1.2 Л1.3Л2.1 Л2.2	0	ситуационное задание
2.5	Криптографические алгоритмы с открытым ключом /Лаб/	3	2	ИД-1.ПК-5 ИД-2.ПК-5 ИД-3.ПК-5	Л1.1 Л1.2 Л1.3Л2.1 Л2.2	0	
2.6	Электронная цифровая подпись /Лаб/	3	2	ИД-1.ПК-5 ИД-2.ПК-5 ИД-3.ПК-5	Л1.1 Л1.2 Л1.3Л2.1 Л2.2	0	
2.7	Криптографические протоколы /Лаб/	3	2	ИД-1.ПК-5 ИД-2.ПК-5 ИД-3.ПК-5	Л1.1 Л1.2 Л1.3Л2.1 Л2.2	0	
2.8	Совершенно секретные системы /Лаб/	3	2	ИД-1.ПК-5 ИД-2.ПК-5 ИД-3.ПК-5	Л1.1 Л1.2 Л1.3Л2.1 Л2.2	0	
2.9	Применение инженерно-технических средств обеспечения информационной безопасности /Пр/	3	1	ИД-1.ПК-5 ИД-2.ПК-5 ИД-3.ПК-5	Л1.1 Л1.2 Л1.3Л2.1 Л2.2	0	ролевая игра
2.10	Виды и основные характеристики шифров. Имитостойкость и помехоустойчивость. /Пр/	3	1	ИД-1.ПК-5 ИД-2.ПК-5 ИД-3.ПК-5	Л1.1 Л1.2 Л1.3Л2.1 Л2.2	0	
2.11	Криптографические системы с секретным и открытым ключом /Пр/	3	1	ИД-1.ПК-5 ИД-2.ПК-5 ИД-3.ПК-5	Л1.1 Л1.2 Л1.3Л2.1 Л2.2	0	кластер
2.12	Электронная цифровая подпись /Пр/	3	2	ИД-1.ПК-5 ИД-2.ПК-5 ИД-3.ПК-5	Л1.1 Л1.2 Л1.3Л2.1 Л2.2	0	кластер
2.13	Конечные поля /Ср/	3	7	ИД-1.ПК-5 ИД-2.ПК-5 ИД-3.ПК-5	Л1.1 Л1.2 Л1.3Л2.1 Л2.2	0	
2.14	Дискретный логарифм /Ср/	3	7	ИД-1.ПК-5 ИД-2.ПК-5 ИД-3.ПК-5	Л1.1 Л1.2 Л1.3Л2.1 Л2.2	0	
2.15	Простые числа. Задача целочисленной факторизации /Ср/	3	11	ИД-1.ПК-5 ИД-2.ПК-5 ИД-3.ПК-5	Л1.1 Л1.2 Л1.3Л2.1 Л2.2	0	
2.16	Эллиптические кривые /Ср/	3	10	ИД-1.ПК-5 ИД-2.ПК-5 ИД-3.ПК-5	Л1.1 Л1.2 Л1.3Л2.1 Л2.2	0	
2.17	Криптография, основанная на эллиптических кривых /Ср/	3	12	ИД-1.ПК-5 ИД-2.ПК-5 ИД-3.ПК-5	Л1.1 Л1.2 Л1.3Л2.1 Л2.2	0	
	Раздел 3. Промежуточная аттестация (зачёт)						
3.1	Подготовка к зачёту /ЗачётСОц/	3	8,85	ИД-1.ПК-5 ИД-2.ПК-5 ИД-3.ПК-5		0	
3.2	Контактная работа /КСРАтт/	3	0,15	ИД-1.ПК-5 ИД-2.ПК-5 ИД-3.ПК-5		0	

5. ФОНД ОЦЕНОЧНЫХ СРЕДСТВ

5.1. Контрольные вопросы и задания

Вопросы к теоретическому зачёту

1. Структура информационной сферы, характеристика ее элементов.
2. Информация как объект правоотношений, категории информации.

3. Система правовой защиты информации.
4. Понятие и виды защищаемой информации.
5. Особенности государственной тайны как защищаемой информации.
6. Система защиты государственной тайны.
7. Засекречивание информации, отнесенной к государственной тайне.
8. Защита сведений отнесенных к государственной тайне.
9. Понятие информации конфиденциального характера.
10. Основные виды конфиденциальной информации, в соответствии с требованиями российской нормативно-правовой базы.
11. Правовой режим конфиденциальной информации.
12. Основные требования, предъявляемые к организации защиты конфиденциальной информации.
13. Понятие и характеристика служебной тайны.
14. Нормативно - правовые основы защиты служебной тайны.
15. Порядок обращения с документами, содержащими служебную информацию ограниченного распространения.
16. Правовые основы защиты коммерческой тайны.
17. Виды информации, составляющей коммерческую тайну.
18. Права и обязанности обладателя коммерческой тайны.
19. Основные угрозы коммерческой тайны.
20. Правовая защита коммерческой тайны.
21. Правовые основы защиты банковской тайны.
22. Раскрытие информации, относящейся к банковской тайне.
23. Нарушение банковской тайны и ответственность за подобные нарушения.
24. Нотариальная тайна и ее особенности. Тайна завещания.
25. Врачебная тайна и ее особенности.
26. Адвокатская тайна и ее особенности.
27. Тайна страхования и ее особенности.
28. Тайна связи и ее особенности. Тайна переписки, почтовых, телеграфных и иных сообщений.
29. Тайна усыновления (удочерения). Тайна исповеди.
30. Формирование российского законодательства в области защиты персональных данных.
31. Основные понятия и содержание закона РФ «О персональных данных».
32. Подзаконные нормативно-правовые документы о порядке правовой защиты персональных данных.
33. Государственный надзор и контроль обработки персональных данных, ответственность за нарушения российского законодательства в данной области.
34. Правовые основы лицензирования в области защиты информации.
35. Правовые основы сертификации в области защиты информации.
36. Особенности правонарушений в информационной сфере.
37. Преступления в сфере компьютерной информации: виды, состав.
38. Основы расследования преступлений в сфере компьютерной информации.
39. Правовая защита информационных систем.
40. Правовая защита результатов интеллектуальной деятельности.
41. Соотношение организационных мер защиты информации с мерами правового и технического характера.
42. Основные термины, связанные с организацией защиты информации.
43. Организационные меры, направленные на защиту государственной тайны.
44. Режим секретности как основной порядок деятельности в сфере защиты государственной тайны.
45. Особенности системы организационной защиты государственной тайны.
46. Распределение между уровнями государственного управления полномочий, управленческих функций и задач по защите государственной тайны.
47. Организация деятельности режимно-секретных органов.
48. Установление и изменение степени секретности сведений, отнесенных к государственной тайне.
49. Понятие «рассекречивание сведений». Основания для рассекречивания сведений.
50. Порядок допуска и доступа к государственной тайне. Основные принципы допускной работы.
51. Номенклатура должностей работников, подлежащих оформлению на допуск и порядок ее составления и утверждения.
52. Документальное оформление для отправки на согласование.
53. Процедура оформления и переоформления допусков и ее документирование, подлежащее согласованию с органами государственной безопасности.
54. Организация доступа к сведениям, составляющим государственную тайну.
55. Понятие «охрана». Цели и задачи охраны.
56. Объекты охраны: территория, здания, помещения, персонал, информационные ресурсы, материальные и финансовые ценности. Особенности их охраны.
57. Виды, способы и особенности охраны различных объектов.
58. Понятие о рубежах охраны. Многорубежная система охраны.
59. Факторы выбора методов и средств охраны.
60. Организация охраны объектов защиты в процессе их транспортировки.
61. Понятие «режим», цели и задачи режимных мероприятий. Виды режима.
62. Организация пропускного режима. Основные положения инструкции об организации пропускного режима и работе бюро пропусков.
63. Виды пропускных документов.

64. Порядок организации работы бюро пропусков.
65. Контрольно-пропускные пункты, их оборудование и организация работы.
66. Понятие «внутриобъектовый режим» и его общие требования.
67. Противопожарный режим и его обеспечение.
68. Подбор и расстановка кадров.
69. Направления и методы работы с персоналом, обладающим конфиденциальной информацией. Организация обучения персонала.
70. Основные формы обучения и методы контроля знаний.
71. Мотивация персонала к выполнению требований по защите информации.
72. Основные формы воздействия на персонал как методы мотивации: вознаграждение, управление карьерой, профессиональная этика.
73. Организация контроля соблюдения персоналом требований режима защиты информации. Методы проверки персонала.
74. Организация служебного расследования по фактам разглашения персоналом конфиденциальной информации.
75. Организационные меры по защите информации при увольнении сотрудника.
76. Основные требования, предъявляемые к подготовке и проведению конфиденциальных переговоров.
77. Основные этапы проведения конфиденциальных переговоров.
78. Подготовка помещения для проведения конфиденциальных переговоров.
79. Подготовка программы проведения конфиденциальных переговоров.
80. Порядок проведения конфиденциальных переговоров.
81. Требования режима защиты информации при приеме в организации посетителей. Поря-док доступа посетителей и командированных лиц к конфиденциальной информации. Порядок пребывания посетителей на территории и в помещениях организации.
82. Требования к программе приема иностранных представителей.
83. Требования к помещениям, в которых проводится прием иностранных представителей.
84. Обеспечение защиты информации при выезде за рубеж командируемых лиц.
85. Основные виды и формы рекламы. Общие требования режима защиты информации в процессе рекламной деятельности.
86. Основные методы защиты информации в рекламной деятельности. Понятие «публикация в открытой печати». Общие требования режима защиты конфиденциальной информации при опубликовании материалов в открытой печати.
87. Особенности защиты информации при опубликовании материалов, определяемые характером деятельности организации, целями публикации, содержанием и характером публикации.
88. Концепция безопасности предприятия (организации) и ее содержание. Политика информационной безопасности.
89. Подразделения, обеспечивающие информационную безопасность предприятия: основные функции, содержание деятельности, структура, обязанности сотрудников.
90. Основные документы службы информационной безопасности.
91. Концепция инженерно-технической защиты информации
92. Утечка информации по техническим каналам
93. Основные принципы инженерно-технической защиты информации
94. Организационные основы инженерно-технической защиты информации
95. Технические средства добывания информации
96. Оценка угрозы утечки информации по техническим каналам и подавление опасных сигналов
97. Методы противодействия утечке и добыванию информации
98. Физические основы утечки информации по каналам побочных электромагнитных излучений и наводок
99. Моделирование процессов инженерно-технической защиты информации
100. Криптографическая система. Схема, основные понятия и принципы построения.
101. Классические шифры: классификация и примеры.
102. Шифры гаммирования.
103. Классическая и Обобщенная алгебраическая модель шифра. Вероятностная модель шифра.
104. Теоретическая стойкость шифров. Совершенные и близкие к совершенным шифры.
105. Композиционные шифры: принципы синтеза и основные схемы.
106. Алгоритм DES.
107. Лавинный эффект блочных шифров и принципы построения S-блоков.
108. Режимы работы блочных шифров: электронная кодовая книга и сцепление блоков шифр-текста.
109. Режимы работы блочных шифров: обратная связь по шифр-тексту.
110. Режимы работы блочных шифров: обратная связь по выходу и режим счетчика.
111. Алгоритм "Магма" ГОСТ Р 34.12-2015 (ГОСТ 28147-89).
112. Алгоритм "Кузнечик" ГОСТ Р 34.12-2015.
113. Режимы работы отечественных блочных шифров ГОСТ Р 34.13-2015.
114. Практическая стойкость криптоалгоритмов.
115. Цели и классификация атак на алгоритмы шифрования.
116. Методы криптоанализа: «грубой силы» и «встреча посередине».
117. Методы криптоанализа: линейный, дифференциальный криптоанализ и его модификации.
118. Методы криптоанализа: слайдовая атака и атака на связанных ключах.
119. Атаки на шифраторы, использующие утечки по побочным каналам.
120. Требования, предъявляемые к современным симметричным алгоритмам шифрования.
121. Ключевые пространства, слабые и эквивалентные ключи, проблемы слабых процедур расширения ключа.
122. Алгоритм AES: основные характеристики и процедура шифрования.

123. Алгоритм AES: процедура прямой расшифровки и процедура расширения ключа.
124. Имитостойкость и помехоустойчивость шифров.
125. Одноключевые хэш-функции. Криптографические контрольные суммы MAC, HMAC.
126. Управление криптографическими ключами: цели управления, иерархия ключей, жизненный цикл ключей, хранение и распределение ключей.
127. Управление криптографическими ключами: методы генерации криптографически сильных ключей.
128. Вопросы организации сетей засекреченной связи.
129. Формирование управляющих последовательностей с помощью регистров сдвига с линейными обратными связями.
130. Способы повышения качества формирования гаммы с помощью регистров сдвига: применение фильтрующих, комбинирующих генераторов, композиций регистров сдвига.
131. Типы криптосистем по ключу. Симметричные и асимметричные криптосистемы: основные принципы и свойства.
132. Система распределения ключей Диффи-Хеллмана.
133. Алгоритм быстрого возведения в степень по модулю.
134. Числа, обратные по модулю. Условие существования. Расширенный алгоритм Евклида, вычисление числа, обратного по модулю.
135. Криптосистема Эль-Гамаля.
136. Криптосистема RSA.
137. Требования к параметрам и атаки на шифр RSA.
138. Бесключевые хэш-функции. Область применения и требования к безопасности.
139. Стандарт бесключевой хэш-функции ГОСТ Р 34.11-2012.
140. Схемы цифровой подписи криптографических систем с открытыми ключами. Детерминированная электронная подпись RSA.
141. Рандомизированная электронная подпись Эль-Гамаля.
142. Криптографические протоколы: типы и решаемые задачи.
143. Криптографические протоколы: протокол разрешения споров по электронной подписи.
144. Криптографические протоколы распределения ключей (симметричная и асимметричная схемы).
145. Криптографические протоколы: атаки на асимметричные схемы и методы противодействия.
146. Криптографические протоколы: протокол Нидхема-Шредера (взаимная аутентификация, асимметричная схема).
147. Эллиптические кривые: определение, вид, уравнение, операции с точками.
148. Эллиптические кривые: применение в криптографии, выбор параметров эллиптических кривых для целей криптографии.
149. Стандарт цифровой подписи на эллиптических кривых ГОСТ Р 34.10-2012.
150. Нормативно-правовые документы и государственные органы исполнительной власти, регламентирующие применение методов и средств криптографической защиты информации в государственных информационных системах.
151. Лицензирование и сертификация в сфере криптографической защиты информации.
152. Цель и сфера применения Федерального закона Российской Федерации «Об электронной цифровой подписи»; основные понятия, введённые законом.
153. Основные положения Федерального закона Российской Федерации «Об электронной цифровой подписи» об условиях использования электронной цифровой подписи.

5.2. Темы письменных работ

Темы сообщений и докладов

1. Информационная безопасность профессиональной деятельности организации.
2. Организационно-правовое обеспечение информационной безопасности бизнеса.
3. Защита информации предприятия от утечки по техническим каналам.
4. Организация информационной безопасности в коммерческом секторе.
5. Организация системы безопасности корпоративных информационных систем.
6. Инженерно-техническая безопасность предприятия.
7. Международно-правовые аспекты информационной безопасности.
8. Информационная собственность и ее защита.
9. Информационные правоотношения, возникающие при создании и применении информационных систем, их сетей, средств обеспечения и механизмов информационной безопасности.
10. Информационные угрозы предпринимательству.
11. Особенности информационной безопасности банков.
12. Классификация возможных угроз безопасности. Существующие способы устранения угроз.
13. Компьютерные преступления, правоустанавливающие акты, взаимоотношения предприятия и правоохранительных органов.
14. Методы защиты корпоративной информации.
15. Основные направления обеспечения безопасности коммерческого предприятия.
16. Защита персональных данных на предприятии.
17. Аудит информационной безопасности.
18. Роль информационной безопасности в сфере электронной торговли.
19. Комплексный подход к созданию системы защиты информации на предприятии.
20. Угрозы информационной безопасности в таможенном секторе.
21. Международная информационная безопасность.
22. Выявление рисков нарушения информационной безопасности предприятия.

23. Защита информационной среды на предприятии. 24. Обеспечение безопасного доступа к информационным ресурсам организации. 25. Экономика информационной безопасности предприятия. 26. Комплексная информационная безопасность объекта. 27. Информационная безопасность организации и персонал. 28. Правовой статус и функции службы безопасности по обеспечению информационной безопасности бизнеса.
5.3. Фонд оценочных средств
Формируется отдельным документом в соответствии с Положением о фонде оценочных средств ГАГУ

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	Скрипник Д.А.	Общие вопросы технической защиты информации: учебное пособие	Москва: Интернет-Университет Информационных Технологий (ИНТУИТ), 2020	http://www.iprbookshop.ru/89451.html
Л1.2	Тюльпинова Н.В.	Защита интеллектуальной собственности и компьютерной информации: учебное пособие для магистров	Саратов: Вузовское образование, 2020	http://www.iprbookshop.ru/88755.htm
Л1.3	Шаньгин В.Ф.	Информационная безопасность и защита информации: учебное пособие	Саратов: Профобразование, 2019	http://www.iprbookshop.ru/87995.html

6.1.2. Дополнительная литература

	Авторы, составители	Заглавие	Издательство, год	Эл. адрес
Л2.1	Басалова Г.В.	Основы криптографии: учебное пособие	Москва: Интернет-Университет Информационных Технологий (ИНТУИТ), Ай Пи Ар Медиа, 2020	http://www.iprbookshop.ru/89455.html
Л2.2	Сычев А.М., Ревенков П.В., Дудка А.Б.	Безопасность электронного банкинга: учебник	Москва: ЦИПСиР, Ай Пи Эр Медиа, 2019	http://www.iprbookshop.ru/86159.html

6.3.1 Перечень программного обеспечения	
6.3.1.1	MS Office
6.3.1.2	Kaspersky Endpoint Security для бизнеса СТАНДАРТНЫЙ
6.3.1.3	MS WINDOWS
6.3.1.4	NVDA
6.3.1.5	Google Chrome
6.3.1.6	Яндекс.Браузер
6.3.2 Перечень информационных справочных систем	
6.3.2.1	База данных «Электронная библиотека Горно-Алтайского государственного университета»
6.3.2.2	Электронно-библиотечная система IPRbooks
6.3.2.3	КонсультантПлюс
6.3.2.4	Межвузовская электронная библиотека

7. ОБРАЗОВАТЕЛЬНЫЕ ТЕХНОЛОГИИ

	ролевая игра	
	кластер	
	круглый стол	
	ситуационное задание	

8. МАТЕРИАЛЬНО-ТЕХНИЧЕСКОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ (МОДУЛЯ)		
Номер аудитории	**Назначение**	**Основное оснащение**
106 А2	Учебная аудитория для проведения занятий лекционного типа, занятий семинарского типа, курсового проектирования (выполнения курсовых работ), групповых и индивидуальных консультаций, текущего контроля и промежуточной аттестации.	Рабочее место преподавателя. Посадочные места обучающихся (по количеству обучающихся). Интерактивная доска с проектором, компьютер, ученическая доска, презентационная трибуна, подключение к интернету, шкафы
317 А2	Компьютерный класс, класс деловых игр, центр (класс) деловых игр, класс имитации деятельности предприятия, лаборатория имитации деятельности предприятия, учебно-тренинговый центр (лаборатория), лаборатория информационно-коммуникативных технологий. 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). Интерактивная доска с проектором, экран, подключение к интернету, ученическая доска, презентационная трибуна

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 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.