

МИНОБРНАУКИ РОССИИ

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

Информационная безопасность рабочая программа дисциплины (модуля)

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

Учебный план 09.03.03_2022_822.plx
09.03.03 Прикладная информатика
Прикладная информатика в экономике

Квалификация **бакалавр**

Форма обучения **очная**

Общая трудоемкость **3 ЗЕТ**

Часов по учебному плану 108
в том числе:
аудиторные занятия 44
самостоятельная работа 54,3
часов на контроль 8,85

Виды контроля в семестрах:
зачеты с оценкой 8

Распределение часов дисциплины по семестрам

Семестр (<Курс>.<Семестр на курсе>)	8 (4.2)		Итого	
	10			
Неделя				
Вид занятий	УП	РП	УП	РП
Лекции	14	14	14	14
Лабораторные	20	20	20	20
Практические	10	10	10	10
Консультации (для студента)	0,7	0,7	0,7	0,7
Контроль самостоятельной работы при проведении аттестации	0,15	0,15	0,15	0,15
В том числе инт.	4	4	4	4
Итого ауд.	44	44	44	44
Контактная работа	44,85	44,85	44,85	44,85
Сам. работа	54,3	54,3	54,3	54,3
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

Информационная безопасность

разработана в соответствии с ФГОС:

Федеральный государственный образовательный стандарт высшего образования - бакалавриат по направлению подготовки 09.03.03 Прикладная информатика (приказ Минобрнауки России от 19.09.2017 г. № 922)

составлена на основании учебного плана:

09.03.03 Прикладная информатика

утвержденного учёным советом вуза от 27.01.2022 протокол № 1.

Рабочая программа утверждена на заседании кафедры

кафедра экономики, туризма и прикладной информатики

Протокол от 21.04.2022 протокол № 9

Зав. кафедрой Куттубаева Тосканай Айтмуқановна



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 Айтмуқановна

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 Айтмуқановна

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 Айтмуқановна

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 Айтмуқановна

1. ЦЕЛИ И ЗАДАЧИ ОСВОЕНИЯ ДИСЦИПЛИНЫ

1.1	<i>Цели:</i> Формирование знаний по основным уровням информационной безопасности, происхождению угроз, развитие умений применения современных методов и технологий защиты информации на ПК и в сетях, антивирусное программное обеспечение, методов шифрования информации; развитие творческих навыков при решении сложных научно-технических задач, связанных с обеспечением информационной безопасности личности, общества и государства
1.2	<i>Задачи:</i> <ul style="list-style-type: none"> • развить и дополнить знания студентов, полученных в результате изучения других предметов, по основам защиты информации; • рассмотреть понятие внешних и внутренних угроз, направленных на компьютерную систему; • рассмотреть уровни безопасности компьютерных систем и дать представление об современных методах защиты информации на соответствующих уровнях; • рассмотреть понятие вируса и его функциональные возможности; • изучить антивирусное программное обеспечение и получить навыки работы с ним; • рассмотреть современные технологии шифрования информации. • рассмотреть вопросы обеспечения информационной безопасности личности, общества и государства;

2. МЕСТО ДИСЦИПЛИНЫ В СТРУКТУРЕ ООП

Цикл (раздел) ООП:	Б1.О
2.1	Требования к предварительной подготовке обучающегося:
2.2	Дисциплины и практики, для которых освоение данной дисциплины (модуля) необходимо как предшествующее:

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

ОПК-3: Способен решать стандартные задачи профессиональной деятельности на основе информационной и библиографической культуры с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности;
ИД-1.ОПК-3: Определяет принципы, методы и средства решения стандартных задач профессиональной деятельности с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности.
основные требования информационной безопасности. основные законодательные и нормативно-правовые акты
ИД-2.ОПК-3: Решает стандартные задачи профессиональной деятельности на основе информационной и библиографической культуры с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности
решает стандартные задачи профессиональной деятельности с учетом принципов информационной безопасности. умеет использовать ПО для обеспечения информационной безопасности информационных систем
ИД-3.ОПК-3: Владеет навыками подготовки обзоров, аннотаций, составления рефератов, научных докладов, публикаций и библиографии по научно-исследовательской работе с учетом требований информационной безопасности
подготовки обзоров и сравнений технических характеристик ПО навыками составления рефератов и докладов с учетом требований информационной безопасности.

4. СТРУКТУРА И СОДЕРЖАНИЕ ДИСЦИПЛИНЫ (МОДУЛЯ)

Код занятия	Наименование разделов и тем /вид занятия/	Семестр / Курс	Часов	Компетенции	Литература	Инте ракт.	Примечание
	Раздел 1. Модуль 2						

1.1	<p>Программно-технический аспект ИБ. Вирусы и антивирусы</p> <p>Программно-технический аспект ИБ. Понятие вируса как вредоносной программы. Структура, функционал вируса, предметы и цели, примеры реальных вирусных атак. Понятие антивирусной программы, как автоматизированного средства борьбы с вирусами. Поиск, уничтожение вирусов. Классификация антивирусного ПО.</p> <p>Демонстрация работы с ПО. Таблицы сравнительной характеристики ПО /Ср/</p>	8	10	ИД-1.ОПК-3 ИД-2.ОПК-3 ИД-3.ОПК-3	Л1.1 Л1.2 Л1.3 Л2.1 Л2.2 Л2.3 Л2.4 Л2.5	0	
1.2	Защита информации от несанкционированного доступа /Лек/	8	2	ИД-1.ОПК-3 ИД-2.ОПК-3 ИД-3.ОПК-3	Л1.1 Л1.2 Л1.3 Л2.1 Л2.2 Л2.3 Л2.4 Л2.5	0	
1.3	Защита информации от несанкционированного доступа /Пр/	8	2	ИД-1.ОПК-3 ИД-2.ОПК-3 ИД-3.ОПК-3	Л1.1 Л1.2 Л1.3 Л2.1 Л2.2 Л2.3 Л2.4 Л2.5	0	
1.4	<p>Защита информации от несанкционированного доступа</p> <p>Система защиты информации от несанкционированного доступа «Страж NT»</p> <p>Система защиты информации от несанкционированного доступа «Dallas Lock»</p> <p>Система защиты информации «Secret NET 5.0-C» /Лаб/</p>	8	20	ИД-1.ОПК-3 ИД-2.ОПК-3 ИД-3.ОПК-3	Л1.1 Л1.2 Л1.3 Л2.1 Л2.2 Л2.3 Л2.4 Л2.5	4	
1.5	<p>Защита информации от несанкционированного доступа</p> <p>Отчеты по лабораторным работам /Ср/</p>	8	11	ИД-1.ОПК-3 ИД-2.ОПК-3 ИД-3.ОПК-3	Л1.1 Л1.2 Л1.3 Л2.1 Л2.2 Л2.3 Л2.4 Л2.5	0	
1.6	<p>Технологии обеспечения ИБ. Криптография и шифрование.</p> <p>Идентификация и аутентификация пользователей. Методы разграничения доступа. Регистрация и аудит ИС. Межсетевое экранирование. Понятие шифров и кодов. Эволюция методов шифрования и кодирования информации. Механические, аппаратные и программные криптографические средства. Электронная цифровая подпись. /Лек/</p>	8	4	ИД-1.ОПК-3 ИД-2.ОПК-3 ИД-3.ОПК-3	Л1.1 Л1.2 Л1.3 Л2.1 Л2.2 Л2.3 Л2.4 Л2.5	0	

1.7	Технологии обеспечения ИБ. Криптография и шифрование. Симметричные криптосистемы (шифры перестановки), шифры простой и сложной замены (система шифрования Цезаря, шифр Гронсфелда, шифры многоалфавитной замены), гаммирование, асимметричные криптосистемы, схема шифрования Эль Гамаля. /Пр/	8	4	ИД-1.ОПК-3 ИД-2.ОПК-3 ИД-3.ОПК-3	Л1.1 Л1.2 Л1.3Л2.1 Л2.2 Л2.3 Л2.4 Л2.5	0	
1.8	Технологии обеспечения ИБ. Криптография и шифрование. Выполнение домашнего задания /Ср/	8	10	ИД-1.ОПК-3 ИД-2.ОПК-3 ИД-3.ОПК-3	Л1.1 Л1.2 Л1.3Л2.1 Л2.2 Л2.3 Л2.4 Л2.5	0	
Раздел 2. Модуль 1							
2.1	Информационные угрозы и уровни обеспечения безопасности Внешние и внутренние угрозы; природного и человеческого характера; умышленные и неумышленные; угрозы на программном, аппаратном и механическом уровне. Компоненты ИБ: доступность, целостность, конфиденциальность. Уровни (аспекты) обеспечения ИБ: законодательно-правовой; административно-организационный; программно-технический. Формирование режима ИБ /Лек/	8	2	ИД-1.ОПК-3 ИД-2.ОПК-3 ИД-3.ОПК-3	Л1.1 Л1.2 Л1.3Л2.1 Л2.2 Л2.3 Л2.4 Л2.5	0	
2.2	Информационные угрозы и уровни обеспечения безопасности конспект /Ср/	8	6	ИД-1.ОПК-3 ИД-2.ОПК-3 ИД-3.ОПК-3	Л1.1 Л1.2 Л1.3Л2.1 Л2.2 Л2.3 Л2.4 Л2.5	0	
2.3	Законодательно-правовой аспект. Информационное законодательство Понятие информационного общества и информационного законодательства. Основные положения закона РФ о защите информации: понятие информации, владельцы информации, уровни информационного взаимодействия. Нарушения в информационной сфере. Понятие Государственной тайны. /Лек/	8	4	ИД-1.ОПК-3 ИД-2.ОПК-3 ИД-3.ОПК-3	Л1.1 Л1.2 Л1.3Л2.1 Л2.2 Л2.3 Л2.4 Л2.5	0	
2.4	Законодательно-правовой аспект. Информационное законодательство Нормативно-правовые акты. Работа с системами Гарант, Консультант, Изучение ГОСТов /Пр/	8	4	ИД-1.ОПК-3 ИД-2.ОПК-3 ИД-3.ОПК-3	Л1.1 Л1.2 Л1.3Л2.1 Л2.2 Л2.3 Л2.4 Л2.5	0	
2.5	Законодательно-правовой аспект. Информационное законодательство Выписки из законодательных и нормативно-правовых актов /Ср/	8	6	ИД-1.ОПК-3 ИД-2.ОПК-3 ИД-3.ОПК-3	Л1.1 Л1.2 Л1.3Л2.1 Л2.2 Л2.3 Л2.4 Л2.5	0	

2.6	Административно-организационный аспект. Политика ИБ предприятия Цели, задачи и содержание административного уровня обеспечения ИБ предприятия. Разработка политики ИБ предприятия. Подготовка кадров. Проведение анализа угроз. Расчет и страхование рисков. /Лек/	8	2	ИД-1.ОПК-3 ИД-2.ОПК-3 ИД-3.ОПК-3	Л1.1 Л1.2 Л1.3 Л2.1 Л2.2 Л2.3 Л2.4 Л2.5	0	
2.7	Административно-организационный аспект. Политика ИБ предприятия Выписки из законодательных и нормативно-правовых актов /Ср/	8	11,3	ИД-1.ОПК-3 ИД-2.ОПК-3 ИД-3.ОПК-3	Л1.1 Л1.2 Л1.3 Л2.1 Л2.2 Л2.3 Л2.4 Л2.5	0	
Раздел 3. Промежуточная аттестация (зачёт)							
3.1	Подготовка к зачёту /ЗачётСОц/	8	8,85	ИД-1.ОПК-3 ИД-2.ОПК-3 ИД-3.ОПК-3	Л1.2 Л1.3 Л2.3 Л2.4 Л2.5	0	
3.2	Контактная работа /КСРАтт/	8	0,15	ИД-1.ОПК-3 ИД-2.ОПК-3 ИД-3.ОПК-3	Л1.2 Л1.3 Л2.3 Л2.4 Л2.5	0	
Раздел 4. Консультации							
4.1	Консультация по дисциплине /Конс/	8	0,7	ИД-1.ОПК-3 ИД-2.ОПК-3 ИД-3.ОПК-3	Л1.2 Л1.3 Л2.3 Л2.4 Л2.5	0	

5. ФОНД ОЦЕНОЧНЫХ СРЕДСТВ

5.1. Контрольные вопросы и задания

Законодательно-правовой уровень защиты информации
Права собственника информации
Понятие государственной тайны
Основные положения закона РФ о защите информации
Защита информации на административном уровне
Разграничение доступа сотрудников при работе в информационной системе
Идентификация и аутентификация
Правила формирования паролей
Роль менеджера предприятия в организации защиты информации. Политика безопасности.
Программный уровень защиты информации.
Защита прикладного программного обеспечения
Защита операционной системы
Аппаратный уровень защиты информации
Физический уровень защиты информации
Защита информации в локальных сетях.
Защита информации в сети Интернет
Возможные способы защиты типового офиса: один сервер, несколько рабочих станций и выход в Интернет
Понятие вируса, его функциональные возможности
Классификация вирусов
Антивирусное программное обеспечение, его функции
Методика изучения ПО. Сравнительный анализ известных антивирусных программ
Сетевые антивирусные фильтры
Использование буферных компьютеров для фильтрации вирусов
Шифрование и кодирование как способ защиты информации
Понятие цифровой подписи, методы использования

5.2. Темы письменных работ

1. Сравнение зарубежного и отечественного законодательств по защите информации.

2. Внешние средства защиты информационных комплексов. 3. От отдельных программ к комплексным мерам защиты информации. 4. Вирусы: классификация, функциональность. 5. Сравнительная характеристика антивирусных программ. 6. Защита информации в сетях. 7. Особенности защиты информации в крупных информационных предприятиях, таких как банки. 8. Сравнительная характеристика методов шифрования информации. 9. Методы защиты от взломщиков. 10. Защита от нежелательных сообщений (спам) в Интернет. 11. Информационная защита операционных систем. 12. Способы защиты баз данных. 13. Криптографические алгоритмы. 14. Защита информации в ГАГУ. 15. Защита информации в социальных сетях. 16. Законодательно-правовой аспект ИБ.
5.3. Фонд оценочных средств
ФОСы хранятся отдельным документом
5.4. Перечень видов оценочных средств

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	Фомин Д. В.	Защита информации: специализированные аттестованные программные и программно- аппаратные средства:	Саратов: Вузовское образование, 2021	https://www.iprbookshop.ru/110329.html
Л1.3	Ревнивых А. В.	Информационная безопасность в организациях: учебное пособие	Москва: Ай Пи Ар Медиа, 2021	https://www.iprbookshop.ru/108227.html
6.1.2. Дополнительная литература				
	Авторы, составители	Заглавие	Издательство, год	Эл. адрес
Л2.1	Бисюков В.М.	Защита и обработка конфиденциальных документов: учебное пособие	Ставрополь: Северо-Кавказский федеральный университет, 2016	www.iprbookshop.ru/66019.html
Л2.2	Голиков А.М.	Основы проектирования защищенных телекоммуникационных систем: учебное пособие	Томск: Томский государственный университет систем управления и радиоэлектроники, 2016	www.iprbookshop.ru/72158.html
Л2.3	Матвеева Л.Г., Никитаева А.Ю., Чернова О.А., Маслюкова Е.В.	Информационная экономика: учебник	Ростов-на-Дону: Издательство Южного федерального университета, 2018	http://www.iprbookshop.ru/87714.html
Л2.4	Голембиовская О. М., Рыгов М. Ю., Шинаков [и др.] К. Е.	Этапы формирования модели угроз и модели нарушителя информационной безопасности с учетом изменений законодательства Российской Федерации: учебное пособие	Саратов: Вузовское образование, 2021	https://www.iprbookshop.ru/109162.html
Л2.5	Костин В. Н.	Методы и средства защиты компьютерной информации: криптографические методы для защиты информации: учебное пособие	Москва: Издательский Дом МИСиС, 2018	https://www.iprbookshop.ru/98201.html
6.3.1 Перечень программного обеспечения				
6.3.1.1	Kaspersky Endpoint Security для бизнеса СТАНДАРТНЫЙ			

6.3.1.2	MS Office
6.3.1.3	Google Chrome
6.3.1.4	NVDA
6.3.1.5	VMware Player
6.3.1.6	MS Windows
6.3.2 Перечень информационных справочных систем	
6.3.2.1	КонсультантПлюс
6.3.2.2	Гарант

7. ОБРАЗОВАТЕЛЬНЫЕ ТЕХНОЛОГИИ	
	проблемная лекция
	ситуационное задание

8. МАТЕРИАЛЬНО-ТЕХНИЧЕСКОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ (МОДУЛЯ)		
Номер аудитории	Назначение	Основное оснащение
320 А2	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, ученическая доска, подключение к сети Интернет

9. МЕТОДИЧЕСКИЕ УКАЗАНИЯ ДЛЯ ОБУЧАЮЩИХСЯ ПО ОСВОЕНИЮ ДИСЦИПЛИНЫ (МОДУЛЯ)
<p>1. Методические указания по самостоятельной работе студента</p> <p>Самостоятельная работа призвана способствовать развитию у студентов творческих навыков, инициативы, умению организовать свое время.</p> <p>При выполнении плана самостоятельной работы студенту необходимо изучить теоретический материал, представленный в рекомендуемой литературе, творчески его переработать и представить его для отчета в форме, рекомендованной в приведенной ниже таблице.</p> <p>Работа студента должна быть полной, раскрывающей уровень освоения студентом той или иной темы и грамотно оформленной, показывающей творческий и инициативный подход студента к выполнению задания.</p> <p>Выполненные задания проверяются преподавателем и оцениваются в баллах.</p> <p>Задания для самостоятельной работы выполняются студентом в письменном виде на стандартных листах формата А4.</p> <p>Методические указания по подготовке рефератов (докладов)</p> <p>Реферат — письменная работа объемом 10-18 печатных страниц, представляющая собой краткое точное изложение сущности какого-либо вопроса, темы на основе одной или нескольких книг, монографий или других первоисточников. Реферат должен содержать основные фактические сведения и выводы по рассматриваемому вопросу. Помимо реферирования прочитанной литературы, от студента требуется аргументированное изложение собственных мыслей по рассматриваемому вопросу. В реферате нужны развернутые аргументы, рассуждения, сравнения. Материал подается не столько в развитии, сколько в форме констатации или описания. Содержание реферлируемого произведения излагается объективно от имени автора.</p> <p>Структура реферата:</p> <ol style="list-style-type: none"> 1. Титульный лист 2. После титульного листа на отдельной странице следует оглавление (план, содержание), в котором указаны названия всех разделов (пунктов плана) реферата и номера страниц, указывающие начало этих разделов в тексте реферата. 3. После оглавления следует введение. Объем введения составляет 1,5-2 страницы. 4. Основная часть реферата может иметь одну или несколько глав, состоящих из 2-3 параграфов (подпунктов, разделов) и предполагает осмысленное и логичное изложение главных положений и идей, содержащихся в изученной литературе. В тексте обязательны ссылки на первоисточники. В том случае если цитируется или используется чья-либо неординарная мысль, идея, вывод, приводится какой-либо цифровой материал, таблицу - обязательно сделайте ссылку на того автора у кого вы взяли данный материал. 5. Заключение содержит главные выводы, и итоги из текста основной части, в нем отмечается, как выполнены задачи и достигнуты ли цели, сформулированные во введении. 6. Приложение может включать графики, таблицы, расчеты. 7. Библиография (список литературы) здесь указывается реально использованная для написания реферата литература. Список составляется согласно правилам библиографического описания. <p>Требования, предъявляемые к оформлению реферата.</p> <p>Объемы рефератов колеблются от 10-18 машинописных страниц. Работа выполняется на одной стороне листа стандартного формата. По обеим сторонам листа оставляются поля размером 35 мм. слева и 15 мм. справа, рекомендуется шрифт 12-14, интервал - 1,5. Все листы реферата должны быть пронумерованы. Каждый вопрос в тексте должен иметь заголовки в</p>

точном соответствии с наименованием в плане-оглавлении.

Методические указания по подготовке конспектов

При подготовке конспектов необходимо использовать различные способы конспектирования, особенности которых раскрываются ниже.

Тезисы — это кратко сформулированные основные мысли, положения изучаемого материала, которые лаконично выражают суть рассматриваемого текста, дают возможность раскрыть его содержание. Приступая к освоению записи в виде тезисов, полезно в самом тексте отмечать места, наиболее четко формулирующие основную мысль, которую автор доказывает (если, конечно, это не библиотечная книга). Часто такой отбор облегчается шрифтовым выделением, сделанным в самом тексте. **Линейно-последовательная запись текста.** При конспектировании линейно — последовательным способом целесообразно использование плакатно-оформительских средств, которые включают в себя следующие: сдвиг текста конспекта по горизонтали, по вертикали; выделение жирным (или другим) шрифтом особо значимых слов; использование различных цветов; подчеркивание; заключение в рамку главной информации.

Способ «вопросов - ответов». Он заключается в том, что, поделив страницу тетради пополам вертикальной чертой, конспектирующий в левой части страницы самостоятельно формулирует вопросы или проблемы, затронутые в данном тексте, а в правой части дает ответы на них. Одна из модификаций способа «вопросов - ответов» — таблица, где место вопроса занимает формулировка проблемы, поднятой автором (лектором), а место ответа - решение данной проблемы. Иногда в таблице могут появиться и дополнительные графы: например, «мое мнение» и т.п.

Схема с фрагментами — способ конспектирования, позволяющий ярче выявить структуру текста, — при этом фрагменты текста (опорные слова, словосочетания, пояснения всякого рода) в сочетании с графикой помогают созданию рационально-лаконичного конспекта.

Простая схема — способ конспектирования, близкий к схеме с фрагментами, объяснений к которой конспектирующий не пишет, но должен уметь давать их устно. Этот способ требует высокой квалификации конспектирующего. В противном случае такой конспект нельзя будет использовать. Наиболее распространенными являются схемы типа "генеалогическое дерево" и "паучок". В схеме "генеалогическое дерево" выделяют основные составляющие более сложного понятия, ключевые слова и т. п. и располагаются в последовательности "сверху - вниз" - от общего понятия к его частным составляющим. В схеме "паучок" записывается название темы или вопроса и заключается в овал, который составляет "тело паучка". Затем нужно продумать, какие из входящих в тему понятий являются основными и записать их в схеме так, что они образуют "ножки паука". Для того чтобы усилить его устойчивость, нужно присоединить к каждой "ножке" ключевые слова или фразы, которые служат опорой для памяти.

Действия при составлении конспекта - схемы могут быть такими: 1. Подберите факты для составления схемы. 2. Выделите среди них основные, общие понятия. 3. Определите ключевые слова, фразы, помогающие раскрыть суть основного понятия. 4. Сгруппируйте факты в логической последовательности. 5. Дайте название выделенным группам. 6. Заполните схему данными.

Параллельный способ конспектирования. Конспект оформляется на двух листах параллельно или один лист делится вертикальной чертой пополам и записи делаются в правой и в левой части листа. Однако лучше использовать разные способы конспектирования для записи одного и того же материала.

Комбинированный конспект — вершина овладения рациональным конспектированием. При этом умело используются все перечисленные способы, сочетая их в одном конспекте (один из видов конспекта свободно перетекает в другой в зависимости от конспектируемого текста, от желания и умения конспектирующего). Именно при комбинированном конспекте более всего проявляется уровень подготовки и индивидуальность студента.

Опорный конспект. В опорном конспекте содержание информации "кодируется" с помощью сочетания графических символов, знаков, рисунков, ключевых слов, цифр и т. п.