

Федеральное государственное бюджетное образовательное учреждение
высшего образования
"Дальневосточный государственный университет путей сообщения"
(ДВГУПС)

УТВЕРЖДАЮ

Зав.кафедрой

(к206) Автоматика, телемеханика и связь

Годяев А.И., д-р техн.
наук, доцент



17.06.2021

РАБОЧАЯ ПРОГРАММА

дисциплины **Основы криптографии с открытыми ключами**

для направления подготовки 11.03.02 Инфокоммуникационные технологии и системы связи

Составитель(и): к.т.н., доцент, Бондарь К. М.

Обсуждена на заседании кафедры: (к206) Автоматика, телемеханика и связь

Протокол от 16.06.2021г. № 7

Обсуждена на заседании методической комиссии учебно-структурного подразделения: Протокол от 17.06.2021 г. № 6

Визирование РПД для исполнения в очередном учебном году

Председатель МК РНС

__ _____ 2023 г.

Рабочая программа пересмотрена, обсуждена и одобрена для исполнения в 2023-2024 учебном году на заседании кафедры (к206) Автоматика, телемеханика и связь

Протокол от __ _____ 2023 г. № __
Зав. кафедрой Годяев А.И., д-р техн. наук, доцент

Визирование РПД для исполнения в очередном учебном году

Председатель МК РНС

__ _____ 2024 г.

Рабочая программа пересмотрена, обсуждена и одобрена для исполнения в 2024-2025 учебном году на заседании кафедры (к206) Автоматика, телемеханика и связь

Протокол от __ _____ 2024 г. № __
Зав. кафедрой Годяев А.И., д-р техн. наук, доцент

Визирование РПД для исполнения в очередном учебном году

Председатель МК РНС

__ _____ 2025 г.

Рабочая программа пересмотрена, обсуждена и одобрена для исполнения в 2025-2026 учебном году на заседании кафедры (к206) Автоматика, телемеханика и связь

Протокол от __ _____ 2025 г. № __
Зав. кафедрой Годяев А.И., д-р техн. наук, доцент

Визирование РПД для исполнения в очередном учебном году

Председатель МК РНС

__ _____ 2026 г.

Рабочая программа пересмотрена, обсуждена и одобрена для исполнения в 2026-2027 учебном году на заседании кафедры (к206) Автоматика, телемеханика и связь

Протокол от __ _____ 2026 г. № __
Зав. кафедрой Годяев А.И., д-р техн. наук, доцент

Рабочая программа дисциплины Основы криптографии с открытыми ключами
разработана в соответствии с ФГОС, утвержденным приказом Министерства образования и науки Российской Федерации от 19.09.2017 № 930

Квалификация **бакалавр**

Форма обучения **очная**

ОБЪЕМ ДИСЦИПЛИНЫ (МОДУЛЯ) В ЗАЧЕТНЫХ ЕДИНИЦАХ С УКАЗАНИЕМ КОЛИЧЕСТВА АКАДЕМИЧЕСКИХ ЧАСОВ, ВЫДЕЛЕННЫХ НА КОНТАКТНУЮ РАБОТУ ОБУЧАЮЩИХСЯ С ПРЕПОДАВАТЕЛЕМ (ПО ВИДАМ УЧЕБНЫХ ЗАНЯТИЙ) И НА САМОСТОЯТЕЛЬНУЮ РАБОТУ ОБУЧАЮЩИХСЯ

Общая трудоемкость **3 ЗЕТ**

Часов по учебному плану	108	Виды контроля в семестрах:
в том числе:		экзамены (семестр) 6
контактная работа	38	РГР 6 сем. (1)
самостоятельная работа	34	
часов на контроль	36	

Распределение часов дисциплины по семестрам (курсам)

Семестр (<Курс>.<Семес тр на курсе>)	6 (3.2)		Итого	
	16 5/6			
Неделя	16 5/6			
Вид занятий	УП	РП	УП	РП
Лекции	16	16	16	16
Практические	16	16	16	16
Контроль самостоятельной работы	6	6	6	6
В том числе инт.	16	16	16	16
Итого ауд.	32	32	32	32
Контактная работа	38	38	38	38
Сам. работа	34	34	34	34
Часы на контроль	36	36	36	36
Итого	108	108	108	108

1. АННОТАЦИЯ ДИСЦИПЛИНЫ (МОДУЛЯ)

1.1	Изучение вопросов основ криптографической защиты информации в телекоммуникационных системах. Фундаментализация, интенсификация и индивидуализация процесса обучения криптографии путём внедрения и эффективного использования достижений кибернетики и теории связи.
-----	--

2. МЕСТО ДИСЦИПЛИНЫ (МОДУЛЯ) В СТРУКТУРЕ ОБРАЗОВАТЕЛЬНОЙ ПРОГРАММЫ

Код дисциплины:	Б1.В.05
2.1	Требования к предварительной подготовке обучающегося:
2.1.1	Высшая математика
2.1.2	Основы технической эксплуатации сетей связи
2.2	Дисциплины и практики, для которых освоение данной дисциплины (модуля) необходимо как предшествующее:
2.2.1	Согласно ОПОП не требуется

3. ПЕРЕЧЕНЬ ПЛАНИРУЕМЫХ РЕЗУЛЬТАТОВ ОБУЧЕНИЯ ПО ДИСЦИПЛИНЕ (МОДУЛЮ), СООТНЕСЕННЫХ С ПЛАНИРУЕМЫМИ РЕЗУЛЬТАТАМИ ОСВОЕНИЯ ОБРАЗОВАТЕЛЬНОЙ ПРОГРАММЫ

УК-2: Способен определять круг задач в рамках поставленной цели и выбирать оптимальные способы их решения, исходя из действующих правовых норм, имеющихся ресурсов и ограничений
Знать: Виды ресурсов и ограничений для решения профессиональных задач; основные методы оценки разных способов решения задач; действующее законодательство и правовые нормы, регулирующие профессиональную деятельность.
Уметь: Проводить анализ поставленной цели и формулировать задачи, которые необходимо решить для ее достижения; анализировать альтернативные варианты для достижения намеченных результатов; использовать нормативно-правовую документацию в сфере профессиональной деятельности.
Владеть: Методиками разработки цели и задач проекта; методами оценки потребности в ресурсах, продолжительности и стоимости проекта; навыками работы с нормативно-правовой документацией.

ПК-6: Способен оценивать параметры безопасности и защиты программного обеспечения и сетевых устройств администрируемой сети с помощью специальных средств управления безопасностью

Знать: Архитектуру, протоколы и общие принципы функционирования аппаратных, программных и программно-аппаратных средств администрируемой сети основные принципы, криптографические протоколы и программные средства обеспечения информационной безопасности сетевых устройств.
Уметь: Применять программные, аппаратные и программно-аппаратные средства защиты сетевых устройств от несанкционированного доступа пользоваться нормативно-технической документацией в области обеспечения информационной безопасности инфокоммуникационных систем.
Владеть: Навыками и средствами установки и управления специализированными программными средствами защиты сетевых устройств администрируемой сети от несанкционированного доступа.

4. СОДЕРЖАНИЕ ДИСЦИПЛИНЫ (МОДУЛЯ), СТРУКТУРИРОВАННОЕ ПО ТЕМАМ (РАЗДЕЛАМ) С УКАЗАНИЕМ ОТВЕДЕННОГО НА НИХ КОЛИЧЕСТВА АКАДЕМИЧЕСКИХ ЧАСОВ И ВИДОВ УЧЕБНЫХ ЗАНЯТИЙ

Код занятия	Наименование разделов и тем /вид занятия/	Семестр / Курс	Часов	Компетенции	Литература	Инте ракт.	Примечание
	Раздел 1. Лекции						
1.1	Лекция 1. Математический базис криптосистем с открытым ключом. Введение в курс. Основные понятия и определения. Модульная арифметика. Теорема Ферма. Теорема Эйлера.	6	2	УК-2 ПК-6	Л1.1 Л1.2Л2.1 Л2.2 Э1 Э2 Э3 Э4 Э5	2	лекции с запланированы ми ошибками

1.2	Лекция 2. Математический базис криптосистем с открытым ключом. Факторизация, возведение в степень логарифмирование Конечные поля, способы представления. Оценки сложности вычислений. Квадратичные вычеты и тестирование простых чисел /Лек/	6	2	УК-2 ПК-6	Л1.1 Л1.2Л2.1 Л2.2 Э1 Э2 Э3 Э4 Э5	0	
1.3	Лекция 3. Системы шифрования с открытыми ключами. Криптосистемы Эль-Гамала, РША, Рабина, Мас-Элис. Генерирование ключей, шифрование, дешифрование. Атаки на криптосистемы. /Лек/	6	2	УК-2 ПК-6	Л1.1 Л1.2Л2.1 Л2.2 Э1 Э2 Э3 Э4 Э5	2	лекции с запланированы ми ошибками
1.4	Лекция 4. Системы электронной цифровой подписи. Построение криптосистем на основе эллиптических кривых. Бесключевые хэшфункции. /Лек/	6	2	УК-2 ПК-6	Л1.1 Л1.2Л2.1 Л2.2 Э1 Э2 Э3 Э4 Э5	0	
1.5	Лекция 5. Системы электронной цифровой подписи. Модель электронной цифровой подписи сообщения, виды ЭЦП. ЭЦП на основе различных криптосистем. Стандарты ЭЦП и хэш-функции. /Лек/	6	2	УК-2 ПК-6	Л1.1 Л1.2Л2.1 Л2.2 Э1 Э2 Э3 Э4 Э5	2	лекции с запланированы ми ошибками
1.6	Лекция 6. Криптографические протоколы. Обзор основных протоколов. Изучение протоколов разделения секрета, аутентификация пользователей с нулевым разглашением, секретные совместные вычисления, тайное голосование. /Лек/	6	2	УК-2 ПК-6	Л1.1 Л1.2Л2.1 Л2.2 Э1 Э2 Э3 Э4 Э5	0	
1.7	Лекция 7. Управление открытыми ключами. Принцип построения инфраструктуры открытых ключей (РКИ), назначение и использование сертификатов открытых ключей. /Лек/	6	2	УК-2 ПК-6	Л1.1 Л1.2Л2.1 Л2.2 Э1 Э2 Э3 Э4 Э5	2	лекции с запланированы ми ошибками
1.8	Лекция 8. Управление открытыми ключами. Распределение ключей для симметричных систем на основе криптографии с открытыми ключами /Лек/	6	2	УК-2 ПК-6	Л1.1 Л1.2Л2.1 Л2.2 Э1 Э2 Э3 Э4 Э5	0	
Раздел 2. Практические							
2.1	1. Основы теории чисел /Пр/	6	2	УК-2 ПК-6	Л1.1 Л1.2Л2.1 Л2.2 Э1 Э2 Э3 Э4 Э5	2	работа в малых группах
2.2	2. Анализ бесключевой хэш- функции /Пр/	6	2	УК-2 ПК-6	Л1.1 Л1.2Л2.1 Л2.2 Э1 Э2 Э3 Э4 Э5	0	

2.3	3. Методика настройки защищенного обмена с использованием криптографических преобразований на основе программы PGP. /Пр/	6	2	УК-2 ПК-6	Л1.1 Л1.2Л2.1 Л2.2 Э1 Э2 Э3 Э4 Э5	2	работа в малых группах
2.4	4. Изучение криптопротокола с разделением секретных данных между пользователями /Пр/	6	4	УК-2 ПК-6	Л1.1 Л1.2Л2.1 Л2.2 Э1 Э2 Э3 Э4 Э5	0	
2.5	5. Методика использования сертификатов открытых ключей в PKI. /Пр/	6	2	УК-2 ПК-6	Л1.1 Л1.2Л2.1 Л2.2 Э1 Э2 Э3 Э4 Э5	2	работа в малых группах
2.6	6. Методика настройки корневого центра сертификации PKI /Пр/	6	2	УК-2 ПК-6	Л1.1 Л1.2Л2.1 Л2.2 Э1 Э2 Э3 Э4 Э5	0	
2.7	7. Методика создания и распределения открытых ключей пользователей на основе программы PGP. /Пр/	6	2	УК-2 ПК-6	Л1.1 Л1.2Л2.1 Л2.2 Э1 Э2 Э3 Э4 Э5	2	работа в малых группах
Раздел 3. Самостоятельная работа							
3.1	Выполнение РГР /Ср/	6	14	УК-2 ПК-6	Л1.1 Л1.2Л2.1 Л2.2 Э1 Э2 Э3 Э4 Э5	0	
3.2	Изучение литературы и подготовка к экзамену /Ср/	6	12	УК-2 ПК-6	Л1.1 Л1.2Л2.1 Л2.2 Э1 Э2 Э3 Э4 Э5	0	
3.3	Подготовка к практическим занятиям /Ср/	6	8	УК-2 ПК-6	Л1.1 Л1.2Л2.1 Л2.2 Э1 Э2 Э3 Э4 Э5	0	
Раздел 4. Контроль							
4.1	Экзамен /Экзамен/	6	36	УК-2 ПК-6	Л1.1 Л1.2Л2.1 Л2.2 Э1 Э2 Э3 Э4 Э5	0	

5. ОЦЕНОЧНЫЕ МАТЕРИАЛЫ ДЛЯ ПРОВЕДЕНИЯ ПРОМЕЖУТОЧНОЙ АТТЕСТАЦИИ

Размещены в приложении

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

6.1. Рекомендуемая литература

6.1.1. Перечень основной литературы, необходимой для освоения дисциплины (модуля)

	Авторы, составители	Заглавие	Издательство, год
Л1.1	Бутакова Н.Г., Федоров Н.В.	Криптографические методы и средства защиты информации: учеб. пособие для вузов	Санкт-Петербург: Интермедия, 2017,
Л1.2	Мартынов Л. М.	Алгебра и теория чисел для криптографии: учебное пособие	Санкт-Петербург: Лань, 2020, https://e.lanbook.com/book/140740

6.1.2. Перечень дополнительной литературы, необходимой для освоения дисциплины (модуля)

	Авторы, составители	Заглавие	Издательство, год
--	---------------------	----------	-------------------

	Авторы, составители	Заглавие	Издательство, год
Л2.1	Бугакова Н.Г., Фёдоров Н.В.	Криптографические методы и средства защиты информации: учеб. пособие для вузов	Санкт-Петербург: Интермедия, 2016,
Л2.2	Майстренко Н. В., Майстренко А. В.	Основы теории информации и криптографии: учебное электронное издание: учебное пособие	Тамбов: ФГБОУ ВПО "ТГТУ", 2018, http://biblioclub.ru/index.php?page=book&id=570354

6.2. Перечень ресурсов информационно-телекоммуникационной сети "Интернет", необходимых для освоения дисциплины (модуля)

Э1	Научная электронная библиотека eLIBRARY.RU.	http://elibrary.ru/
Э2	Единое окно доступа к образовательным ресурсам.	http://window.edu.ru/
Э3	Журнал "Электросвязь"	http://www.elsv.ru/
Э4	Журнал «CONNECT. Мир информационных технологий»	https://www.connect-wit.ru/izdaniya-connect.html
Э5	Журнал «Автоматика, связь, информатика»	https://asi-journal-rzd.ru/

6.3 Перечень информационных технологий, используемых при осуществлении образовательного процесса по дисциплине (модулю), включая перечень программного обеспечения и информационных справочных систем (при необходимости)

6.3.1 Перечень программного обеспечения

АСТ тест - Комплекс программ для создания банков тестовых заданий, организации и проведения сеансов тестирования, лиц.АСТ.РМ.А096.Л08018.04, дог.372

Free Conference Call (свободная лицензия)

6.3.2 Перечень информационных справочных систем

Профессиональная база данных, информационно-справочная система Гарант - <http://www.garant.ru>

Профессиональная база данных, информационно-справочная система КонсультантПлюс - <http://www.consultant.ru>

Профессиональная база данных, информационно-справочная система Техэксперт - <http://www.cntd.ru>

Научная электронная библиотека eLIBRARY.RU <http://elibrary.ru>

Электронный каталог НТБ ДВГУПС <http://ntb.festu.khv.ru/>

Справочно-правовая система «Кодекс» [Электронный ресурс]. <https://kodeks.ru/>

7. ОПИСАНИЕ МАТЕРИАЛЬНО-ТЕХНИЧЕСКОЙ БАЗЫ, НЕОБХОДИМОЙ ДЛЯ ОСУЩЕСТВЛЕНИЯ ОБРАЗОВАТЕЛЬНОГО ПРОЦЕССА ПО ДИСЦИПЛИНЕ (МОДУЛЮ)

Аудитория	Назначение	Оснащение
303	Учебная аудитория для проведения лабораторных занятий, групповых и индивидуальных консультаций, текущего контроля и промежуточной аттестации. Лаборатория "Системы передачи и защиты дискретной информации. ДВ сетевая академия CISCO"	комплект учебной мебели, компьютеры, мониторы, блок питания - 48/80, Патп-панель, коммутатор cisco safalyst 3560, коммутатор cisco safalyst 35666, коммутатор cisco safalyst 2960, маршрутизатор cisco 2800, маршрутизатор cisco 2801, коммутатор ZyxeL Ies-1000, мужсетевой экран cisco, АКВ
304	Учебная аудитория для проведения занятий лекционного типа	комплект учебной мебели: столы, стулья, интерактивная доска, мультимедийный проектор, компьютер, система акустическая
307	Учебная аудитория для проведения лабораторных и практических занятий, групповых и индивидуальных консультаций, текущего контроля и промежуточной аттестации. Лаборатория "Системы управления, передачи и обработки сигналов"	Персональный компьютер с программным обеспечением, установки «Теория электрической связи», стенд «Микропроцессорные технологии» установки «Изучение принципов ВРК(ЦСК-1)», «Изучение ИКМ – кодека(ЦСК-2), Осциллографы С1-112, комплект учебной мебели.
307	Учебная аудитория для проведения лабораторных и практических занятий, групповых и индивидуальных консультаций, текущего контроля и промежуточной аттестации. Лаборатория "Системы управления, передачи и обработки сигналов"	Персональный компьютер с программным обеспечением, установки «Теория электрической связи», стенд «Микропроцессорные технологии» установки «Изучение принципов ВРК(ЦСК-1)», «Изучение ИКМ – кодека(ЦСК-2), Осциллографы С1-112, комплект учебной мебели.
1303	Помещения для самостоятельной работы обучающихся. Читальный зал НТБ	Тематические плакаты, столы, стулья, стеллажи Компьютерная техника с возможностью подключения к сети Интернет, свободному

Аудитория	Назначение	Оснащение
		доступу в ЭБС и ЭИОС.
249	Помещения для самостоятельной работы обучающихся. Читальный зал НТБ	Тематические плакаты, столы, стулья, стеллажи Компьютерная техника с возможностью подключения к сети Интернет, свободному доступу в ЭБС и ЭИОС.
3322	Помещения для самостоятельной работы обучающихся. Читальный зал НТБ	Тематические плакаты, столы, стулья, стеллажи Компьютерная техника с возможностью подключения к сети Интернет, свободному доступу в ЭБС и ЭИОС.
343	Помещения для самостоятельной работы обучающихся. Читальный зал НТБ	Тематические плакаты, столы, стулья, стеллажи. Компьютерная техника с возможностью подключения к сети Интернет, свободному доступу в ЭБС и ЭИОС.
3317	Помещения для самостоятельной работы обучающихся. Читальный зал НТБ	Тематические плакаты, столы, стулья, стеллажи Компьютерная техника с возможностью подключения к сети Интернет, свободному доступу в ЭБС и ЭИОС.

8. МЕТОДИЧЕСКИЕ МАТЕРИАЛЫ ДЛЯ ОБУЧАЮЩИХСЯ ПО ОСВОЕНИЮ ДИСЦИПЛИНЫ (МОДУЛЯ)

1. Планирование и организация времени, необходимого для изучения дисциплины.

Важным условием успешного освоения дисциплины является создание системы правильной организации труда, позволяющей распределить учебную нагрузку равномерно в соответствии с графиком образовательного процесса. Большую помощь в этом может оказать составление плана работы на семестр, месяц, неделю, день. Его наличие позволит подчинить свободное время целям учебы, трудиться более успешно и эффективно. Нужно осуществлять самоконтроль, который является необходимым условием успешной учебы. Все задания, включая вынесенные на самостоятельную работу, рекомендуется выполнять непосредственно после соответствующего аудиторного занятия (лекции, практического занятия), что способствует лучшему усвоению материала, позволяет своевременно выявить и устранить «пробелы» в знаниях, систематизировать ранее пройденный материал, на его основе приступить к овладению новыми знаниями и навыками. Система университетского обучения основывается на рациональном сочетании нескольких видов учебных занятий (в первую очередь, лекций, лабораторных и практических занятий), работа на которых обладает определенной спецификой.

2. Подготовка к лекциям

Знакомство с дисциплиной происходит уже на первой лекции, где от студента требуется не просто внимание, но и самостоятельное оформление конспекта. При работе с конспектом лекций необходимо учитывать тот фактор, что одни лекции дают ответы на конкретные вопросы темы, другие – лишь выявляют взаимосвязи между явлениями, помогая студенту понять глубинные процессы развития изучаемого предмета, как в истории, так и в настоящее время.

Конспектирование лекций – сложный вид вузовской аудиторной работы, предполагающий интенсивную умственную деятельность студента. Конспект является полезным тогда, когда записано самое существенное и сделано это самим обучающимся. Не надо стремиться записать дословно всю лекцию. Такое «конспектирование» приносит больше вреда, чем пользы. Целесообразно вначале понять основную мысль, излагаемую лектором, а затем записать ее. Желательно записывать на одной странице листа или оставляя поля, на которых позднее, при самостоятельной работе с конспектом, можно сделать дополнительные записи, отметить непонятные места.

Конспект лекции лучше подразделять на пункты, соблюдая красную строку. Этому в большой степени будут способствовать вопросы плана лекции, предложенные преподавателям. Следует обращать внимание на акценты, выводы, которые делает лектор, отмечая наиболее важные моменты в лекционном материале замечаниями «важно», «хорошо запомнить» и т.п. Можно делать это и с помощью разноцветных маркеров или ручек, подчеркивая термины и определения.

Целесообразно разработать собственную систему сокращений, аббревиатур и символов. Однако при дальнейшей работе с конспектом символы лучше заменить обычными словами для быстрого зрительного восприятия текста. Работая над конспектом лекций, всегда необходимо использовать не только учебник, но и ту литературу, которую дополнительно рекомендовал лектор. Именно такая серьезная, кропотливая работа с лекционным материалом позволит глубоко овладеть теоретическим материалом.

3. Подготовка к практическим и лабораторным занятиям

Тщательное продумывание и изучение вопросов плана основывается на проработке пройденного материала (материала лекций, практических и лабораторных занятий), а затем изучения обязательной и дополнительной литературы, рекомендованной к данной теме.

Результат такой работы должен проявиться в способности студента свободно ответить на теоретические вопросы практикума, его выступлении и участии в коллективном обсуждении вопросов изучаемой темы, правильном выполнении практических заданий, лабораторных и контрольных работ.

Необходимо понимать, что невозможно во время аудиторных занятий изложить весь материал из-за лимита аудиторных часов, и при изучении дисциплины недостаточно конспектов занятий. Поэтому самостоятельная работа с учебниками, учебными пособиями, научной, справочной литературой, материалами периодических изданий и Интернета является наиболее эффективным методом получения дополнительных знаний, позволяет значительно активизировать процесс овладения информацией, способствует более глубокому усвоению изучаемого материала, формирует у студентов свое отношение к конкретной проблеме.

4. Рекомендации по работе с литературой

Работу с литературой целесообразно начать с изучения общих работ по теме, а также учебников и учебных пособий. Далее рекомендуется перейти к анализу монографий и статей, рассматривающих отдельные аспекты проблем, изучаемых в рамках курса, а также официальных материалов и неопубликованных документов (научно-исследовательские работы, диссертации), в которых могут содержаться основные вопросы изучаемой проблемы.

Работу с источниками надо начинать с ознакомительного чтения, т.е. просмотреть текст, выделяя его структурные единицы. При ознакомительном чтении закладками отмечаются те страницы, которые требуют более внимательного изучения. В зависимости от результатов ознакомительного чтения выбирается дальнейший способ работы с источником. Если для разрешения поставленной задачи требуется изучение некоторых фрагментов текста, то используется метод выборочного чтения. Если в книге нет подробного оглавления, следует обратить внимание ученика на предметные и именные указатели. Избранные фрагменты или весь текст (если он целиком имеет отношение к теме) требуют вдумчивого, неторопливого чтения с «мысленной проработкой» материала. Такое чтение предполагает выделение: 1) главного в тексте; 2) основных аргументов; 3) выводов. Особое внимание следует обратить на то, вытекает тезис из аргументов или нет. Необходимо также проанализировать, какие из утверждений автора носят проблематичный, гипотетический характер и уловить скрытые вопросы.

Понятно, что умение таким образом работать с текстом приходит далеко не сразу. Наилучший способ научиться выделять главное в тексте, улавливать проблематичный характер утверждений, давать оценку авторской позиции – это сравнительное чтение, в ходе которого студент знакомится с различными мнениями по одному и тому же вопросу, сравнивает весомость и доказательность аргументов сторон и делает вывод о наибольшей убедительности той или иной позиции.

Если в литературе встречаются разные точки зрения по тому или иному вопросу из-за сложности прошедших событий и правовых явлений, нельзя их отвергать, не разобравшись. При наличии расхождений между авторами необходимо найти рациональное зерно у каждого из них, что позволит глубже усвоить предмет изучения и более критично оценивать изучаемые вопросы. Знакомясь с особыми позициями авторов, нужно определять их схожие суждения, аргументы, выводы, а затем сравнивать их между собой и применять из них ту, которая более убедительна.

Следующим этапом работы с литературными источниками является создание конспектов, фиксирующих основные тезисы и аргументы. Можно делать записи на отдельных листах, которые потом легко систематизировать по отдельным темам изучаемого курса. Другой способ – это ведение тематических тетрадей-конспектов по одной какой-либо теме. Большие специальные работы монографического характера целесообразно конспектировать в отдельных тетрадях. Здесь важно вспомнить, что конспекты пишутся на одной стороне листа, с полями и достаточным для исправления и ремарок межстрочным расстоянием (эти правила соблюдаются для удобства редактирования). Если в конспектах приводятся цитаты, то непременно должно быть дано указание на источник (автор, название, выходные данные, № страницы). Впоследствии эта информация может быть использована при написании текста реферата или другого задания. Таким образом, при работе с источниками и литературой важно уметь:

- сопоставлять, сравнивать, классифицировать, группировать, систематизировать информацию в соответствии с определенной учебной задачей;
- обобщать полученную информацию, оценивать прослушанное и прочитанное;
- фиксировать основное содержание сообщений; формулировать, устно и письменно, основную идею сообщения; составлять план, формулировать тезисы;
- готовить и презентовать развернутые сообщения типа доклада;
- работать в разных режимах (индивидуально, в паре, в группе), взаимодействуя друг с другом;
- пользоваться реферативными и справочными материалами;
- контролировать свои действия и действия своих товарищей, объективно оценивать свои действия;
- обращаться за помощью, дополнительными разъяснениями к преподавателю, другим студентам;
- пользоваться лингвистической или контекстуальной догадкой, словарями различного характера, различного рода подсказками, опорам в тексте (ключевые слова, структура текста, предваряющая информация и др.);
- использовать при говорении и письме перифраз, синонимичные средства, словоописания общих понятий, разъяснения, примеры, толкования, «словотворчество»
- повторять или перефразировать реплику собеседника в подтверждении понимания его высказывания или вопроса;
- обратиться за помощью к собеседнику (уточнить вопрос, переспросить и др.);
- использовать мимику, жесты (вообще и в тех случаях, когда языковых средств не хватает для выражения тех или иных коммуникативных намерений).

5. Подготовка к промежуточной аттестации

При подготовке к промежуточной аттестации целесообразно:

- внимательно изучить перечень вопросов и определить, в каких источниках находятся сведения, необходимые для ответа на них;
- внимательно прочитать рекомендованную литературу;
- составить краткие конспекты ответов (планы ответов).