

МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ  
ФЕДЕРАЦИИ

Федеральное государственное бюджетное образовательное учреждение  
высшего образования  
«Забайкальский государственный университет»  
(ФГБОУ ВО «ЗабГУ»)

Факультет естественных наук, математики и технологий  
Кафедра Математики и информатики

УТВЕРЖДАЮ:

Декан факультета

Факультет естественных  
наук, математики и  
технологий

Токарева Юлия Сергеевна

« \_\_\_\_ » \_\_\_\_\_ 20 \_\_\_\_  
г.

**РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ (МОДУЛЯ)**

Б1.В.ДВ.03.02 Информационная безопасность и защита информации  
на 72 часа(ов), 2 зачетных(ые) единиц(ы)  
для направления подготовки (специальности) 44.03.01 - Педагогическое образование

составлена в соответствии с ФГОС ВО, утвержденным приказом  
Министерства образования и науки Российской Федерации от  
« \_\_\_\_ » \_\_\_\_\_ 20 \_\_\_\_ г. № \_\_\_\_

Профиль – Информатика и информационные технологии в образовании (для набора 2024)  
Форма обучения: Заочная

# 1. Организационно-методический раздел

## 1.1 Цели и задачи дисциплины (модуля)

Цель изучения дисциплины:

изучения дисциплины: формирование у обучающихся компетенций по обеспечению информационной безопасности при использовании информационных технологий.

Задачи изучения дисциплины:

- ознакомиться с терминологией, основными понятиями и тенденциями развития информационной безопасности;
- дать понятие об информационной защите, уровнях ее организации и реализации;
- рассмотреть нормативно-правовую базу информационной безопасности;
- рассмотреть модели возможных угроз;
- развитие эмоционально-ценностного отношения к деятельности и ее содержанию.

## 1.2. Место дисциплины (модуля) в структуре ОП

Общая трудоемкость дисциплины «Информационная безопасность и защита информации» составляет 72 часов (2 зачетные единицы), лекционные занятия 8 часов, практические занятия 8 часов, самостоятельная работа 56 часов, зачет.

## 1.3. Объем дисциплины (модуля) с указанием трудоемкости всех видов учебной работы

Общая трудоемкость дисциплины (модуля) составляет 2 зачетных(ые) единиц(ы), 72 часов.

Виды занятий	Семестр 10	Всего часов
Общая трудоемкость		72
Аудиторные занятия, в т.ч.	16	16
Лекционные (ЛК)	8	8
Практические (семинарские) (ПЗ, СЗ)	8	8
Лабораторные (ЛР)	0	0
Самостоятельная работа студентов (СРС)	56	56
Форма промежуточной аттестации в семестре	Зачет	0
Курсовая работа (курсовой проект) (КР, КП)		

## 2. Перечень планируемых результатов обучения по дисциплине, соотнесенных с планируемыми результатами освоения образовательной программы

Планируемые результаты освоения образовательной программы		Планируемые результаты обучения по дисциплине
Код и наименование компетенции	Индикаторы достижения компетенции, формируемые в рамках дисциплины	Дескрипторы: знания, умения, навыки и (или) опыт деятельности
УК-2	УК-2.1. Формулирует совокупность взаимосвязанных задач в рамках поставленной цели работы, обеспечивающих ее достижение. Определяет ожидаемые результаты решения поставленных задач	<p>Знать: основные определения понятия «информационная безопасность».</p> <p>Уметь: выбирать и реализовывать оптимальные методы информационных технологий, применение которых способствует формированию личности безопасного поведения</p> <p>Владеть: навыками идентификации основных видов информационной опасности</p>
УК-2	УК-2.2. Проектирует решение конкретной задачи проекта, выбирая оптимальный способ ее решения, исходя из действующих правовых норм и имеющихся ресурсов и ограничений	<p>Знать: идеи подходы и принципы информационной безопасности;</p> <p>Уметь: выбирать и реализовывать оптимальные, формы информационных технологий, применение которых способствует формированию личности безопасного поведения.</p> <p>Владеть: навыками создания педагогически целесообразной и психологически безопасной образовательной среды</p>
УК-2	УК-2.3. Качественно решает конкретные задачи (исследования, проекта, деятельности) за установленное время	<p>Знать: различные виды информационной опасности, угрожающие каждому человеку и сообществам, их свойства и характеристики</p> <p>Уметь: применять информационные технологии для</p>

		<p>защиты информации</p> <p>Владеть: навыками идентификации основных видов информационной опасности и выбором методов защиты от информационной опасности применительно к сфере своей профессиональной деятельности;</p>
УК-2	УК-2.4. Публично представляет результаты решения задач исследования, проекта, деятельности	<p>Знать: методы предвидения и предупреждения влияния факторов информационной опасности и угроз, способы и средства защиты от них в любых условиях применительно к своей профессиональной деятельности</p> <p>Уметь: использовать различное программное обеспечение для достижения цели;</p> <p>Владеть: навыками бесконфликтного общения с различными субъектами педагогического процесса</p>
ПК-1	ПК-1.1. Знает: концептуальные положения и требования к организации образовательного процесса по информатике, определяемые ФГОС общего образования; особенности проектирования образовательного процесса по информатике в образовательном учреждении общего образования, подходы к планированию образовательной деятельности; содержание курса информатики в образовательном учреждении общего образования; формы, методы и средства обучения информатике, современные образовательные технологии, методические закономерности их выбора; особенности частных методик обучения информатике	<p>Знать: государственную политику в области обеспечения информационной безопасности жизнедеятельности; требования нормативных документов Правительства РФ, Минобрнауки России, МЧС России по информационной безопасности; требования к безопасности регламентов в сфере профессиональной деятельности; понятийно-терминологический аппарат в области информационной безопасности образовательного процесса; способы взаимодействия с другими субъектами образовательного процесса</p>
ПК-1	ПК-1.2. Умеет: проектировать	<p>Уметь: находить, анализировать и</p>

	<p>элементы образовательной программы, рабочую программу учителя информатики; формулировать дидактические цели и задачи обучения информатике и реализовать их в образовательном процессе по информатике; планировать, моделировать и реализовывать различные организационные формы в процессе обучения информатике (урок, экскурсию, домашнюю, внеклассную и внеурочную работу); обосновывать выбор методов обучения информатике и образовательных технологий, применять их в образовательной практике, исходя из особенностей содержания учебного материала, возраста и образовательных потребностей обучаемых; планировать и комплексно применять различные средства обучения информатике</p>	<p>оценивать достоверность информации, предоставляемой в сети Интернет; объяснять элементарные способы самозащиты от информационной опасности в конкретных чрезвычайных ситуациях.</p>
ПК-1	<p>ПК-1.3. Владеет: умениями по планированию и проектированию образовательного процесса; методами обучения информатике и современными образовательными технологиями</p>	<p>Владеть: применением практических навыков обеспечения информационной безопасности в опасных ситуациях, возникающих в учебном процессе и повседневной жизни; формами и методами обучения информационной безопасности, в том числе выходящими за рамки учебных занятий: проектная деятельность, эксперименты и т.п.</p>

### 3. Содержание дисциплины

#### 3.1. Разделы дисциплины и виды занятий

##### 3.1 Структура дисциплины для заочной формы обучения

Модуль	Номер раздела	Наименование раздела	Темы раздела	Всего часов	Аудиторные занятия			С Р С
					Л К	П З	Л Р	

						(С З)		
1	1.1	Основные понятия теории информационной безопасности	Предметная область теории информационной безопасности	9	1	1	0	7
	1.2	Основные понятия теории информационной безопасности	Основные принципы построения систем защиты информации	9	1	1	0	7
2	2.1	Информация как объект защиты	Уровни, виды и формы представления информации. Свойства защищаемой информации	9	1	1	0	7
	2.2	Информация как объект защиты	Государственная политика информационной безопасности	9	1	1	0	7
3	3.1	Угрозы информационной безопасности	Анализ и оценка уязвимостей системы. Классификация угроз информационной безопасности.	9	1	1	0	7
	3.2	Угрозы информационной безопасности	Построение систем защиты от угрозы нарушения конфиденциальности	9	1	1	0	7
4	4.1	Построение систем защиты от угрозы нарушения целостности информации и отказа доступа	Защита целостности информации	9	1	1	0	7
	4.2	Построение систем защиты от угрозы нарушения целостности	Политика и модели безопасности	9	1	1	0	7

		информации и отказа доступа						
Итого				72	8	8	0	56

### 3.2. Содержание разделов дисциплины

#### 3.2.1. Лекционные занятия, содержание и объем в часах

Модуль	Номер раздела	Тема	Содержание	Трудоемкость (в часах)
1	1.1	Предметная область теории информационной безопасности	История становления теории информационной безопасности. Систематизация понятий в области защиты информации. Основные термины и определения правовых понятий в области информационных отношений и защиты информации.	1
	1.2	Основные принципы построения систем защиты информации	Основные термины и определения правовых понятий в области информационных отношений и защиты информации. Концепция комплексной защиты информации.	1
2	2.1	Уровни, виды и формы представления информации. Свойства защищаемой информации	Концепция комплексной защиты информации. Уровни представления информации. Основные свойства защищаемой информации. Виды и формы представления информации. Информационные ресурсы	1
	2.2	Государственная политика и информационная безопасность	Информационная безопасность и ее место в системе национальной безопасности Российской Федерации.	1
3	3.1	Анализ и оценка уязвимостей системы. Классификация угроз информационной безопасности.	Анализ и оценка уязвимостей системы. Классификация угроз информационной безопасности. Основные направления и методы реализации угроз.	1
	3.2	Построение	Определение и основные способы	1

		систем защиты от угрозы нарушения конфиденциальности	несанкционированного доступа. Методы защиты от НСД. Организационные методы защиты от НСД. Инженерно-технические методы защиты от НСД. Построение систем защиты от угрозы утечки по техническим каналам.	
4	4.1	Защита целостности информации	Защита целостности информации при хранении, обработке, транспортировке и угрозы нарушения целостности информации на уровне содержания	1
	4.2	Политика и модели безопасности	Субъектно-объектные модели разграничения доступа. Аксиомы политики безопасности. Политика и модели дискреционного доступа. Парольные системы разграничения доступа	1

### 3.2.2. Практические занятия, содержание и объем в часах

Модуль	Номер раздела	Тема	Содержание	Трудоемкость (в часах)
1	1.1	Предметная область теории информационной безопасности	Задачи защиты информации	1
	1.2	Основные принципы построения систем защиты информации	Средства реализации комплексной защиты информации	1
2	2.1	Уровни, виды и формы представления информации. Свойства защищаемой информации	Структура и шкала ценности информации. Классификация информационных ресурсов	1
	2.2	Государственная политика и информационн	Правовой режим информационных ресурсов. Органы обеспечения информационной безопасности и	1



		ой безопасности	защиты информации, их функции и задачи, нормативная деятельность	
3	3.1	Анализ и оценка уязвимостей системы. Классификация угроз информационной безопасности.	Неформальная модель нарушителя	1
	3.2	Построение систем защиты от угрозы нарушения конфиденциальности	Идентификация и аутентификация. Основные направления и цели использования криптографических методов. Защита от угрозы нарушения конфиденциальности на уровне содержания информации	1
4	4.1	Защита целостности информации	Построение систем защиты от угрозы отказа доступа к информации. Построение систем защиты от угрозы отказа доступа к информации.	1
	4.2	Политика и модели безопасности	Политика и модели мандатного доступа. Политика и модели мандатного доступа. Ролевая модель безопасности.	1

### 3.2.3. Лабораторные занятия, содержание и объем в часах

Модуль	Номер раздела	Тема	Содержание	Трудоемкость (в часах)

### 3.3. Содержание материалов, выносимых на самостоятельное изучение

Модуль	Номер раздела	Содержание материалов, выносимого на самостоятельное изучение	Виды самостоятельной деятельности	Трудоемкость (в часах)
1	1.1	Обзор международных стандартов информационной безопасности	отбор, структурирование и представление материала в виде презентационного исследования	7
	1.2	Роль стандартов	отбор, структурирование и	7

		информационной безопасности	представление материала в виде презентационного исследования	
2	2.1	Критерии безопасности компьютерных систем министерства обороны США (Оранжевая книга), TCSEC	отбор, структурирование и представление материала в виде презентационного исследования	7
	2.2	Европейские критерии безопасности информационных технологий (ITSEC)	отбор, структурирование и представление материала в виде презентационного исследования	7
3	3.1	Федеральные критерии безопасности информационных технологий США	отбор, структурирование и представление материала в виде презентационного исследования	7
	3.2	Единые критерии безопасности информационных технологий	отбор, структурирование и представление материала в виде презентационного исследования	7
4	4.1	Группа международных стандартов 270000	отбор, структурирование и представление материала в виде презентационного исследования	7
	4.2	Проект «Информационные войны и информационное противоборство»: • Определение и основные виды информационных войн • Информационно-техническая война • Информационно-психологическая война	Отбор, структурирование и представление материала в виде презентационного исследования, защита проекта	7

#### **4. Фонд оценочных средств для проведения текущей и промежуточной аттестации обучающихся по дисциплине**

Фонд оценочных средств текущего контроля и промежуточной аттестации по итогам освоения дисциплины представлен в приложении.

[Фонд оценочных средств](#)

## 5. Учебно-методическое и информационное обеспечение дисциплины

### 5.1. Основная литература

#### 5.1.1. Печатные издания

1. 1. Вострецова, Е.В. Основы информационной безопасности : учебное пособие для студентов вузов / Е.В. Вострецова.— Екатеринбург : Изд-во Урал. ун-та, 2019.— 204 с.

#### 5.1.2. Издания из ЭБС

1. 2. Внуков А.А. Защита информации : учебное пособие для вузов / А. А. Внуков. - 3-е изд. - Москва : Юрайт, 2022. - 161 с. - (Высшее образование). - URL: <https://urait.ru/bcode/490277> (дата обращения: 12.10.2022).

2. 3. Импортзамещающие технологии обеспечения информационной безопасности и защиты данных [Электронный ресурс]: учебное пособие / Короченцев Д. А., Черкесова Л. В., Ревякина Е. А., Болдырихин Н. В., Сафарьян О. А. - Ростов-на-Дону : Донской ГТУ, 2021. - 335 с. - Книга из коллекции Донской ГТУ - Информатика. - ISBN 978-5-7890-1893-4. - URL: <https://e.lanbook.com/book/237782> (дата обращения: 12.10.2022).

3. 4. Климентьев, К. Е. Введение в защиту компьютерной информации [Электронный ресурс] / Климентьев К. Е. - Самара : СамГУ, 2020. - 183 с. - URL: <https://e.lanbook.com/book/189043> (дата обращения: 12.10.2022).

4. 5. Овчинников А. А. Криптографические методы защиты информации [Электронный ресурс] : учебное пособие / Овчинников А. А. - Санкт-Петербург : ГУАП, 2021. - 133 с. - Книга из коллекции ГУАП - Информатика. - ISBN 978-5-8088-1591-9. - URL: <https://e.lanbook.com/book/216491> (дата обращения: 12.10.2022).

### 5.2. Дополнительная литература

#### 5.2.1. Печатные издания

1.

#### 5.2.2. Издания из ЭБС

1. 1. Волчков В. П. Теория и методы криптографической защиты информации : учебное пособие. Теория и методы криптографической защиты информации. Ч. 1. Ч. 1 / Волчков В. П., Санников В. Г. - Москва : МТУСИ, 2021. - 77 с. - URL: <https://e.lanbook.com/book/215195> (дата обращения: 12.10.2022).

2. 2. Казарин, О.В. Надежность и безопасность программного обеспечения : Учебное пособие для вузов / Казарин О. В., Шубинский И. Б. - Москва : Юрайт, 2022. - 342 с. - (Высшее образование). - URL: <https://urait.ru/bcode/493262> (дата обращения: 07.02.2022). - ISBN 978-5-534-05142-1 : 1059.00.

3. 3. Программно-аппаратные средства защиты информации [Электронный ресурс] : учебно-методическое пособие / Штеренберг С. И., Гельфанд А. М., Рыжаков Д. В., Фатхутдинов Р. А. - Санкт-Петербург : СПбГУТ им. М.А. Бонч-Бруевича, 2017. - 98 с. - URL: <https://e.lanbook.com/book/180093>. (дата обращения: 12.10.2022).

4. 4. Суворова Г.М. Информационная безопасность : учебное пособие для вузов / Г. М. Суворова. - Москва : Юрайт, 2022. - 253 с. - (Высшее образование). - URL:

<https://urait.ru/bcode/496741> (дата обращения: 12.10.2022). - ISBN 978-5-534-13960-0 : 1039.00.

5. 5. Щеглов А.Ю. Защита информации: основы теории : учебник для вузов / А. Ю. Щеглов, К. А. Щеглов. - Москва : Юрайт, 2022. - 309 с. - (Высшее образование). - URL: <https://urait.ru/bcode/490019> (дата обращения: 12.10.2022). - ISBN 978-5-534-04732-5 : 1229.00.

### 5.3. Базы данных, информационно-справочные и поисковые системы

Название	Ссылка
On-line библиотека свободно доступных материалов по информационным технологиям	<a href="http://citforum.ru/">http://citforum.ru/</a>
Журнал «Сети и системы связи»	<a href="http://www.ccc.ru/">http://www.ccc.ru/</a>

### 6. Перечень программного обеспечения

Программное обеспечение общего назначения: ОС Microsoft Windows, Microsoft Office, АBBYY FineReader, ESET NOD32 Smart Security Business Edition, Foxit Reader, АИБС "МераПро".

Программное обеспечение специального назначения:

### 7. Материально-техническое обеспечение дисциплины

Наименование помещений для проведения учебных занятий и для самостоятельной работы обучающихся	Оснащенность специальных помещений и помещений для самостоятельной работы
Учебные аудитории для проведения занятий лекционного типа	Состав оборудования и технических средств обучения указан в паспорте аудитории, закрепленной расписанием по факультету
Учебные аудитории для проведения практических занятий	

### 8. Методические рекомендации по организации изучения дисциплины

Для эффективного освоения материала дисциплины необходимым является выполнение следующих требований:

- обязательное посещение всех лекционных и практических занятий, способствующее системному овладению материалом курса;
- все вопросы соответствующих разделов и тем по дисциплине необходимо фиксировать (на любых носителях информации);
- обязательное выполнение домашних заданий является важнейшим требованием и условием формирования целостного и системного знания по дисциплине;
- обязательность личной активности каждого студента на всех занятиях по дисциплине;

- в случаях неясности каких-либо вопросов, обсуждаемых на занятиях, необходимо задать соответствующие вопросы преподавателю, а не оставлять их непонятыми;
- в случаях пропусков занятий по уважительным причинам студентам предоставляется право подготовки и представления заданий и ответов на вопросы изученного материала, с расчетом на помощь преподавателя в его усвоении;
- в случаях пропусков без уважительной причины студент обязан самостоятельно изучить соответствующий материал;
- необходимым условием является самостоятельность и инициативность студентов при контроле набора баллов по дисциплине для успешного прохождения промежуточной аттестации.

Порядок организации самостоятельной работы студентов

Самостоятельная работа студентов предполагает:

- самостоятельный поиск, обработку (анализ, синтез, обобщение и систематизацию), адаптацию необходимой по дисциплине информации;
- выполнение заданий для самостоятельной работы;
- изучение и усвоение теоретического материала, представленного на лекционных занятиях и в соответствующих литературных источниках (рекомендуемая основная и дополнительная литература);
- самостоятельное изучение отдельных вопросов курса;
- подготовка к практическим и семинарским занятиям, в соответствии с рекомендациями преподавателя (выполнение конкретных заданий, соответствующие организационные действия и т.д.).

Как правило, организация самостоятельной работы предполагает:

- постановку цели;
- составление соответствующего плана;
- поиск, обработку информации;
- представление результатов работы.

Методические рекомендации по отдельным видам учебно-познавательной деятельности студентов

Методические рекомендации при подготовке к практическим занятиям

Для повышения эффективности проведения практических занятий необходимо учитывать все рекомендации по подготовке к ним, которые даются преподавателем в начале каждого модуля (формулируются соответствующие задания, проблемноориентированные вопросы, представляются рекомендации по методике организации 14 различных форм проведения занятий и т.д.). Определенные формы и методы работы на занятиях требуют предварительной самостоятельной подготовки студентов (например, внутригрупповая и межгрупповая дискуссии, ролевые игры, подготовка итогового семестрового проекта и т.д.). Поэтому необходимо фиксировать все рекомендации преподавателя по подготовке к занятиям.

Для эффективного освоения материала дисциплины в ходе практических занятий необходимо выполнение следующих требований:

- четко понимать цели предстоящих занятий (предварительно формулируются преподавателем);
- владеть навыками поиска, обработки, адаптации и презентации необходимого материала;
- уметь четко формулировать и отстаивать собственный взгляд на рассматриваемые проблемные вопросы, который необходимо подкреплять адекватной аргументацией;
- уметь выделять и формулировать противоречия по рассматриваемым проблемам, понимая их источники;
- владеть навыками публичного выступления (логично, ясно и лаконично излагать свои

мысли; адекватно оценивать восприятие и понимание слушателями представляемого материала; отвечать на задаваемые вопросы; приводить адекватные и убедительные аргументы в защиту своей позиции и т.д.);

- уметь критически оценивать собственные знания, умения и навыки в динамике в сравнении с таковыми у других, с целью раскрытия дополнительных возможностей их развития;
- при подготовке к занятиям обязательно изучить рекомендуемую литературу;
- оценить различные точки зрения на проблемные вопросы нескольких исследователей, а не ограничиваться рассмотрением позиции одного автора;
- при формулировке собственной точки зрения предусмотреть убедительную ее аргументацию и возможность возникновения спорных ситуаций;
- владеть навыками работы в команде (при выполнении определенных заданий, предполагающих работу в микрогруппах, при проведении ролевых игр, дискуссий и т.д.).

Семинар – вид практических занятий, предусматривающий самостоятельную проработку студентами отдельных тем и проблем с содержанием учебной дисциплины и последующим представлением и обсуждением результатов этого изучения (в различных формах). Семинары представляют собой своеобразный синтез теоретической подготовки студентов с практической. Основной дидактической целью семинаров выступает оптимальное сочетание лекционных занятий с систематической самостоятельной учебнопознавательной деятельностью студентов. Методические рекомендации при подготовке индивидуальных сообщений (докладов) Данный вид учебно-познавательной деятельности требует от студентов достаточно высокого базового уровня подготовки, большой степени самостоятельности и целого ряда умений и навыков серьезной интеллектуальной работы. Работа по подготовке индивидуальных сообщений и докладов предполагает достаточно длительную системную работу студента, а также в случае необходимости консультативную помощь преподавателя.

Работа должна быть тщательно продумана, спланирована и разделена на соответствующие этапы, каждый из которых требует целого ряда определенных умений и навыков:

- определение и формулировка темы сообщения или доклада (либо осмысление темы, сформулированной преподавателем в соответствующих случаях);
- составление плана с использованием анализа, синтеза, обобщения и логики построения изложения материала;
- определение источников информации;
- работа с источниками научной информации (подбор, анализ, обобщение, систематизация, адаптация и т.д.);
- формулировка основных обобщений и выводов по результатам анализа изученного материала.

Структура сообщения (доклада) может обоснованно варьировать, но в большинстве случаев она предполагает наличие следующих частей: вступления (обозначение актуальности и постановка проблемы), основной части (обзор различных точек зрения на проблему и ее решение), заключения (формулировка соответствующих обобщений, выводов, предположений и перспектив), а в соответствующих случаях – перечня используемых источников информации. Методические рекомендации по подготовке к дискуссии Дискуссия выступает важнейшим средством активизации познавательной деятельности. Как метод активного обучения дискуссия может использоваться как в рамках традиционных (развернутая беседа, система докладов и рефератов), так и новых форм практических занятий (анализ конкретных ситуаций, ролевая игра, круглый стол и т.д.). Выделяется особая форма семинарского занятия – семинар-дискуссия. Различают следующие разновидности семинара-дискуссии:

1. По объему охватываемого материала:

- - фрагментарные дискуссии («мини-дискуссии») (предназначенные для обсуждения какого-то конкретного вопроса и занимающие, как правило, определенную часть занятия);
- - развернутые дискуссии (посвященные изучению раздела (темы) в целом, охватывающие одно или несколько занятий);

2. По реальности существования участников:

- - реальные (предполагающие общение с реальными участниками);
- - воображаемые (предполагающие общение с воображаемым оппонентом (инсценировка спора)).

Организация дискуссии предполагает последовательность определенных этапов:

- - подготовка дискуссии;
- - проведение дискуссии;
- - анализ итогов дискуссии.

Самым важным этапом при этом является подготовка к дискуссии, т.к. все последующие этапы определяются именно качеством предварительной подготовки. Подготовка к дискуссии, как правило, включает следующие составляющие:

- - определение темы дискуссии (тема может быть задана преподавателем, а также обсуждаться и выбираться в процессе изучения материала по критериям наличия противоречий, проблемно-ориентированного характера при высокой актуальности, научной и социальной значимости);
- - определение предмета дискуссии (с тем, чтобы не потерять время на обсуждение второстепенных аспектов проблемы);
- - определение задач дискуссии (для организации целенаправленности, разделения функций участников дискуссии, экономии времени).

Подготовка к дискуссии должна предполагать индивидуальные и групповые консультации, предназначенные для задания целенаправленности дискуссии, а также – для активизации самостоятельной работы студентов. При этом преподавателю необходимо избегать детального разъяснения содержания проблемы, т.к. в этом случае не о чем будет спорить, и дискуссия будет сорвана. Задача преподавателя должна состоять в ненавязчивой помощи участникам будущей дискуссии в определении наличия противоречивых точек зрения на рассматриваемую проблему, порекомендовав изучить первоисточники и дополнительную литературу. Необходимо подчеркнуть особую важность тщательной подготовки к дискуссии самого преподавателя, выступающего в качестве модератора. Цель такой подготовки состоит не только в том, чтобы обрести уверенность при обсуждении научной проблемы, но и в том, чтобы составить ясное представление о качестве подготовки участников дискуссии.

Разработчик/группа разработчиков:  
Татьяна Александровна Гудкова

**Типовая программа утверждена**

Согласована с выпускающей кафедрой  
Заведующий кафедрой

\_\_\_\_\_ «\_\_\_» \_\_\_\_\_ 20\_\_ г.