МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ
Федеральное государственное бюджетное образовательное учреждение
высшего образования
«КУБАНСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ»
Факультет истории, социологии и международных отношений

УТВЕРЖДАЮ:
Проректор по учебной работе,
качеству образования – первый
проректор
_____ Хагуров Т.А.
подпись
«31» мая 2024 г.

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ (МОДУЛЯ)

ФТД.В.01 ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ

(код и наименование дисциплины в соответствии с учебным планом)

Направление подготовки/специальность 39.03.01 Социология
(код и наименование направления подготовки/специальности)

Направленность (профиль) / специализация
Социальная теория и прикладное социальное знание
Прикладные методы в социологических исследованиях
(наименование направленности (профиля) / специализации)

Форма обучения очная
(очная, очно-заочная, заочная)

Квалификация бакалавр

Краснодар 2024

Рабочая программа дисциплины ФТД.В.01 «Информационная безопасность» составлена в соответствии с федеральным государственным образовательным стандартом высшего образования (ФГОС ВО) по направлению подготовки / специальности 39.03.01 Социология

код и наименование направления подготовки

Программу составили:

М.В. Донцова, доцент, канд. социол. наук _____ подпись

Т.А. Рунаев, доцент, канд. социол. наук _____ подпись

Рабочая программа дисциплины ФТД.В.01 «Информационная безопасность» утверждена на заседании кафедры (разработчика) социологии
протокол №10 «16» 03 2024 г.
Заведующий кафедрой (разработчика) Т.А. Хагуров
фамилия, инициалы _____ подпись

Рабочая программа обсуждена на заседании кафедры (выпускающей)
протокол №10 «16» 03 2024 г.
Заведующий кафедрой (выпускающей) Хагуров Т.А.
фамилия, инициалы _____ подпись

Утверждена на заседании учебно-методической комиссии факультета истории, социологии и международных отношений
протокол №6 «15» мая 2024 г.
Председатель УМК факультета Э.Г. Вартаньян
фамилия, инициалы _____ подпись

Рецензенты:

Муха В.Н., кандидат социологических наук, доцент кафедры социологии, правоведения и работы с персоналом ФГБОУ ВО КубГТУ

Юрченко Н.Н., кандидат политических наук, доцент кафедры политологии и политического управления ФГБОУ ВО КубГУ

1 Цели и задачи изучения дисциплины (модуля).

1.1 Цель освоения дисциплины.

Формирование у студентов знаний об основных направлениях исследований в области информационной безопасности, а также развития навыков применения актуальных цифровых методов, предназначенных для анализа состояния информационной безопасности социальных групп и организаций.

1.2 Задачи дисциплины.

Для достижения цели в ходе учебного процесса предполагается решить следующие задачи:

− познакомить студентов с современными социологическими теориями и концепциями информационного общества;

− выработать у студентов навыки сбора, систематизации и обработки информации, необходимой для выявления рисков информационной безопасности социальных групп и организаций;

− развить способность проектирования индивидуального и (или) группового исследования с применением анализа данных для решения проблем информационной безопасности.

1.3 Место дисциплины (модуля) в структуре образовательной программы.

Дисциплина «Информационная безопасность» относится к части факультативных дисциплин учебного плана. Дисциплина рассчитана на слушателей без предварительной подготовки. Необходимо общее знакомство со спецификой профессиональной деятельности, а также знание иностранного языка на уровне, достаточном для изучения рекомендуемых источников.

1.4 Перечень планируемых результатов обучения по дисциплине (модулю), соотнесенных с планируемыми результатами освоения образовательной программы.

Изучение данной учебной дисциплины направлено на формирование у обучающихся профессиональных компетенций:

Код и наименование индикатора	Результаты обучения по дисциплине
ОПК-1. Способен понимать принципы работы современных информационных технологий и использовать их для решения задач профессиональной деятельности	
ОПК-1.6 Знание современных цифровых технологий, возможность их применения для цифровой безопасности, потенциальные риски и способы их нейтрализации.	***знает*** основные программные цифровые решения, необходимые для поддержания информационной безопасности общества и организаций
	умеет ориентироваться в программных цифровых решениях (в частности в пакетах RStudio и библиотеках Python), позволяющих выявлять риски для информационной безопасности
	владеет базовыми навыками программирования на языках R и Python, необходимыми для определения рисков и поддержания информационной безопасности
ОПК-2. Способен к социологическому анализу и научному объяснению социальных явлений и процессов на основе научных теорий, концепций, подходов	
ОПК-2.1 Находит, анализирует и представляет фактические данные, готовит аналитическую информацию об исследуемых социальных группах, процессах и явлениях.	***знает*** методы data mining и text mining, позволяющие проводить анализ числовой и текстовой информации в социальных группах; инструменты поиска информации в отечественных и зарубежных базах данных
	умеет представлять обработанные данные в виде графиков, диаграмм, сетей, иконографики
	владеет навыками создания программных кодов /

	алгоритмов на языках программирования R с целью анализа информации
ОПК-2.2 Описывает социальные исследования и процессы на основе объективной безоценочной интерпретации эмпирических данных	***знает*** правила научной работы при анализе информационной безопасности социальных групп, процессов и явлений
	умеет использовать статистические метрики для описания состояния информационной безопасности групп, процессов и явлений
	владеет основными навыками статистики с целью характеристики информационной безопасности
ОПК-2.3 Объясняет социальные явления и процессы на основе концепций и объяснительных моделей социологии.	***знает*** основные социологические концепции и подходы к исследованию феноменов информационного общества, медиа и цифрового пространства
	умеет подбирать релевантные объяснительные модели для объяснения результатов анализа эмпирических данных
	владеет навыками теоретизирования и генерализации эмпирических / прикладных данных
ПК-2 Способен подготовить проектное предложение для проведения социологического исследования (самостоятельно или под руководством)	
ПК-2.1 Описывает проблемную ситуацию.	***знает*** правила определения проблемной ситуации в рамках проектного социологического исследования
	умеет находить проблемные ситуации в жизнедеятельности сообществ, организаций, медиа каналов
	владеет навыками описания проблемной ситуации с применением научного терминологического аппарата
ПК-2.2 Обосновывает актуальность проекта для решения поставленной проблемы.	***знает*** актуальные социологические теории и концепции, необходимые для обоснования актуальности проблемы информационной безопасности
	умеет ставить цели и задачи для проведения мониторинга информационной безопасности сообществ и организаций
	владеет социологическим инструментарием, необходимым для проведения мониторинга информационной безопасности сообществ и организаций
ПК-2.3 Согласовывает документацию, регламентирующую взаимодействие заказчика и исполнителя социологического исследования.	***знает*** перечень документации социологического исследования; структурные элементы программы социологического исследования
	умеет составлять программу социологического исследования; предлагать релевантные методы решения выявленной проблемы; определять планируемые результаты в виде конечного продукта
	владеет навыками написания отчета социологического исследования

2. Структура и содержание дисциплины.

2.1 Распределение трудоёмкости дисциплины по видам работ.

Общая трудоёмкость дисциплины составляет 2 зач.ед. (72 часа), их распределение по видам работ представлено в таблице (*для студентов ОФО*)

Вид учебной работы	Всего	Семестры			
	часов		(часы)		
		6			

Контактная работа, в том числе:		**34,2**	**34,2**			
Аудиторные занятия (всего):		**32**	**32**			
Занятия лекционного типа		16	16			
Лабораторные занятия		-	-			
Занятия семинарского типа (семинары, практические занятия)		16	16			
Иная контактная работа:						
Контроль самостоятельной работы (КСР)		2	2			
Промежуточная аттестация (ИКР)		0,2	0,2			
Самостоятельная работа, в том числе:		**37,8**	**37,8**			
Курсовая работа		-	-			
Проработка учебного (теоретического) материала		14	14			
Выполнение индивидуальных заданий (подготовка проектов, презентаций)		14	14			
Реферат		9	9			
Подготовка к текущему контролю		0,8	0,8			
Контроль:						
Подготовка к экзамену						
Общая трудоемкость	**час.**	**72**				
	в том числе контактная работа	**34,2**				
	зач.ед	**2**				

2.2 Структура дисциплины:

Распределение видов учебной работы и их трудоемкости по разделам дисциплины.
Разделы дисциплины, изучаемые в 6 семестре *(очная форма)*

№	Наименование разделов	Количество часов				
		Всего	Аудиторная работа			Внеаудиторная работа
			Л	ПЗ	ЛР	СРС
1	2	3	4	5	6	7
1.	Теоретические основания информационной безопасности	12	4	4	-	4
2.	Риски информационного поля	12	4	4	-	4
3.	Законодательство в области информационной безопасности	10	2	2	-	6
4.	Особенности содержания по обеспечению информационной безопасности	10	2	2	-	6
5.	Цифровые методы выявления рисков информационного поля	16	4	4	-	8
	Контроль самостоятельной работы (КСР)	2	-	-	-	-
	Промежуточная аттестация (ИКР)	0,2	-	-	-	-
	Реферат	9	-	-	-	9
	Подготовка к текущему контролю	0,8	-	-	-	0,8

	Итого по дисциплине:	72	16	16	-	37,8

Примечание: Л - лекции, ПЗ - практические занятия / семинары, ЛР - лабораторные занятия, СРС - самостоятельная работа студента

2.3 Содержание разделов дисциплины:

2.3.1 Занятия лекционного типа.

№	Наименование раздела	Содержание раздела	Форма текущего контроля
1	2	3	4
1.	Теоретические основания информационной безопасности	Понятие информации. Эволюция каналов передачи информации. Концепт «глобальной деревни» М. Маклюэна. Теория информационного общества М. Кастельса, концепция четвертой промышленной революции К. Шваба, концепция «второй эры машин» Э. Бринолфссона и Э. МакАфи, сетевая теория современных сообществ М. Грановеттера. Развитие Интернета в России и за рубежом: история возникновения, динамика числа подключенных пользователей. Техносоциальная реальность (пересечение пространственных логик онлайн и оффлайн). Типология сообществ в киберпространстве. Big Data и датификация социальной жизни.	Опрос
2.	Риски информационного поля	Информационная война. Угрозы идеологической безопасности государства. Информационный терроризм / кибертерроризм. Кибербуллинг. Киберсталкинг. Информационные фейки в СМИ. Посягательства на личное информационное пространство. Кибермошенничество.	Опрос
3.	Законодательство в области информационной безопасности	ФЗ «О средствах массовой информации» от 27 декабря 1991 г. ФЗ «О противодействии экстремисткой деятельности» от 25 июля 2002 г. ФЗ «О коммерческой тайне» от 29 июня 2004 г. ФЗ «Об информации, информационных технологиях и о защите информации» от 27 июля 2006 г. ФЗ «О персональных данных» от 27 июля 2006 г. ФЗ «О защите детей от информации, причиняющей вред их здоровью и развитию» от 29 декабря 2010 г. Доктрина информационной безопасности РФ от 5 декабря 2016 г. Стратегия национальной безопасности РФ от 2 июля 2021 г.	Опрос
4.	Особенности содержания по обеспечению информационной безопасности	Процедурный уровень обеспечения информационной безопасности. Компьютерные вирусы и антивирусы. Криптография / шифрование в цифровой среде. Парольная защита. Идентификация и аутентификация. Разграничение доступа. Межсетевые экраны как средство. Защиты несанкционированного доступа. Средства родительского контроля. Цифровая компетентность. Алгоритмическая грамотность.	Опрос

5.	Цифровые методы выявления рисков информационного поля	Пакеты в RStudio. Обзор пакетов интеллектуального анализа текстов. Способы построения авторских словарей тональностей. Алгоритм выявления тональности текста. Описание методов тематического моделирования. Анализ совпадений (co-occurrence): построение сетей терминов. Латентное размещение Дирихле (LDA)	Опрос

2.3.2 Занятия семинарского типа.

№	Наименование раздела	Содержание раздела	Форма текущего контроля
1	2	3	4
1.	Теоретические основания информационной безопасности	Понятие информации. Эволюция каналов передачи информации. Концепт «глобальной деревни» М. Маклюэна. Теория информационного общества М. Кастельса, концепция четвертой промышленной революции К. Шваба, концепция «второй эры машин» Э. Бринолфссона и Э. МакАфи, сетевая теория современных сообществ М. Грановеттера. Развитие Интернета в России и за рубежом: история возникновения, динамика числа подключенных пользователей. Техносоциальная реальность (пересечение пространственных логик онлайн и оффлайн). Типология сообществ в киберпространстве. Big Data и датификация социальной жизни.	Доклады
2.	Риски информационного поля	Информационная война. Угрозы идеологической безопасности государства. Информационный терроризм / кибертерроризм. Кибербуллинг. Киберсталкинг. Информационные фейки в СМИ. Посягательства на личное информационное пространство. Кибермошенничество.	
3.	Законодательство в области информационной безопасности	ФЗ «О средствах массовой информации» от 27 декабря 1991 г. ФЗ «О противодействии экстремисткой деятельности» от 25 июля 2002 г. ФЗ «О коммерческой тайне» от 29 июня 2004 г. ФЗ «Об информации, информационных технологиях и о защите информации» от 27 июля 2006 г. ФЗ «О персональных данных» от 27 июля 2006 г. ФЗ «О защите детей от информации, причиняющей вред их здоровью и развитию» от 29 декабря 2010 г. Доктрина информационной безопасности РФ от 5 декабря 2016 г. Стратегия национальной безопасности РФ от 2 июля 2021 г.	Практическая работа

4.	Особенности содержания по обеспечению информационной безопасности	Процедурный уровень обеспечения информационной безопасности. Компьютерные вирусы и антивирусы. Криптография / шифрование в цифровой среде. Парольная защита. Идентификация и аутентификация. Разграничение доступа. Межсетевые экраны как средство. Защиты несанкционированного доступа. Средства родительского контроля.Цифровая компетентность. Алгоритмическая грамотность.	Практическая работа
5.	Цифровые методы выявления рисков информационного поля	Пакеты в RStudio. Обзор пакетов интеллектуального анализа текстов. Способы построения авторских словарей тональностей. Алгоритм выявления тональности текста. Описание методов тематического моделирования. Анализ совпадений (co-occurrence): построение сетей терминов. Латентное размещение Дирихле (LDA)	Групповой проект

2.3.3 Лабораторные занятия.

Лабораторные занятия - не предусмотрены

2.3.4 Примерная тематика курсовых работ (проектов)

Курсовые работы (проекты) - не предусмотрены

2.4 Перечень учебно-методического обеспечения для самостоятельной работы обучающихся по дисциплине (модулю)

Учебно-методические материалы для самостоятельной работы обучающихся из числа инвалидов и лиц с ограниченными возможностями здоровья (ОВЗ) предоставляются в формах, адаптированных к ограничениям их здоровья и восприятия информации:

Для лиц с нарушениями зрения:

- в печатной форме увеличенным шрифтом,
- в форме электронного документа.

Для лиц с нарушениями слуха:

- в печатной форме,
- в форме электронного документа.

Для лиц с нарушениями опорно-двигательного аппарата:

- в печатной форме,
- в форме электронного документа.

Данный перечень может быть конкретизирован в зависимости от контингента обучающихся.

3. Образовательные технологии.

При реализации различных видов учебной работы по дисциплине «Информационная безопасность», используются следующие образовательные технологии: активные и интерактивные формы проведения занятий - интерактивные и проблемные лекции; опросы; самостоятельная работа - работа с публикациями в предметной области дисциплины; подготовка рефератов, выполнение практических занятий.

Для лиц с ограниченными возможностями здоровья предусмотрена организация консультаций с использованием электронной почты.

4. Оценочные средства для текущего контроля успеваемости и промежуточной аттестации.

Оценочные средства предназначены для контроля и оценки образовательных достижений обучающихся, освоивших программу учебной дисциплины «Информационная безопасность».

Оценочные средства включает контрольные материалы для проведения текущего контроля в форме тестовых заданий, доклада-презентации по проблемным вопросам, разноуровневых заданий, ролевой игры, ситуационных задач и промежуточной аттестации в форме вопросов и заданий к зачету

Структура оценочных средств для текущей и промежуточной аттестации

№ п/п	Код и наименование индикатора	Результат обучения	Наименование оценочного средства	
			Текущий контроль	Промежуточная аттестация
1	ОПК-1.6 Знание современных цифровых технологий, возможность их применения для цифровой безопасности, потенциальные риски и способы их нейтрализации.	***знает*** основные программные цифровые решения, необходимые для поддержания информационной безопасности общества и организаций	контрольный опрос (КО); тестирование (Т)	Вопрос на зачете
		умеет ориентироваться в программных цифровых решениях (в частности в пакетах RStudio и библиотеках Python), позволяющих выявлять риски для информационной безопасности	разработка проекта (РП)	Вопрос на зачете
		владеет базовыми навыками программирования на языках R и Python, необходимыми для определения рисков и поддержания информационной безопасности	доклад с презентацией (ДП)	Вопрос на зачете
2	ОПК-2.1 Находит, анализирует и представляет фактические данные, готовит аналитическую информацию об исследуемых социальных группах, процессах и явлениях.	***знает*** методы data mining и text mining, позволяющие проводить анализ числовой и текстовой информации в социальных группах; инструменты поиска информации в отечественных и зарубежных базах данных	контрольный опрос (КО); тестирование (Т)	Вопрос на зачете
		умеет представлять обработанные данные в виде графиков, диаграмм, сетей, иконографики	разработка проекта (РП)	Вопрос на зачете
		владеет навыками создания программных кодов / алгоритмов на языках	разработка рабочей программы с презентацией	Вопрос на зачете

		программирования R с целью анализа информации	(РПП)	
3	ОПК-2.2 Описывает социальные исследования и процессы на основе объективной безоценочной интерпретации эмпирических данных	***знает*** правила научной работы при анализе информационной безопасности социальных групп, процессов и явлений	контрольный опрос (КО); тестирование (Т)	Вопрос на зачете
		умеет использовать статистические метрики для описания состояния информационной безопасности групп, процессов и явлений	разработка проекта (РП)	Вопрос на зачете
		владеет основными навыками статистики с целью характеристики информационной безопасности	разработка рабочей программы с презентацией (РПП)	Вопрос на зачете
4	ОПК-2.3 Объясняет социальные явления и процессы на основе концепций и объяснительных моделей социологии.	***знает*** основные социологические концепции и подходы к исследованию феноменов информационного общества, медиа и цифрового пространства	контрольный опрос (КО); тестирование (Т)	Вопрос на зачете
		умеет подбирать релевантные объяснительные модели для объяснения результатов анализа эмпирических данных	разработка проекта (РП)	Вопрос на зачете
		владеет навыками теоретизирования и генерализации эмпирических / прикладных данных	разработка рабочей программы с презентацией (РПП)	Вопрос на зачете
5	ПК-2.1 Описывает проблемную ситуацию.	***знает*** правила определения проблемной ситуации в рамках проектного социологического исследования	контрольный опрос (КО); тестирование (Т)	Вопрос на зачете
		умеет находить проблемные ситуации в жизнедеятельности сообществ, организаций, медиа каналов	разработка проекта (РП)	Вопрос на зачете
		владеет навыками описания проблемной ситуации с применением научного терминологического аппарата	разработка рабочей программы с презентацией (РПП)	Вопрос на зачете

6	ПК-2.2 Обосновывает актуальность проекта для решения поставленной проблемы.	***знает*** актуальные социологические теории и концепции, необходимые для обоснования актуальности проблемы информационной безопасности	контрольный опрос (КО); тестирование (Т)	Вопрос на зачете
		умеет ставить цели и задачи для проведения мониторинга информационной безопасности сообществ и организаций	разработка проекта (РП)	Вопрос на зачете
		владеет социологическим инструментарием, необходимым для проведения мониторинга информационной безопасности сообществ и организаций	разработка рабочей программы с презентацией (РПП)	Вопрос на зачете
7	ПК-2.3 Согласовывает документацию, регламентирующую взаимодействие заказчика и исполнителя социологического исследования.	***знает*** перечень документации социологического исследования; структурные элементы программы социологического исследования	контрольный опрос (КО); тестирование (Т)	Вопрос на зачете
		умеет составлять программу социологического исследования; предлагать релевантные методы решения выявленной проблемы; определять планируемые результаты в виде конечного продукта	разработка проекта (РП)	Вопрос на зачете
		владеет навыками написания отчета социологического исследования	разработка рабочей программы с презентацией (РПП)	Вопрос на зачете

4.1 Фонд оценочных средств для проведения промежуточной аттестации.

Вопросы на зачет

1. Характеристики информационной реальности, процесс ее институционализации как фактор общественного прогресса.
2. Современная научно-техническая революция.
3. Информационное неравенство как гуманитарная проблема.

4. Виды информационных угроз.
5. Законодательная база информационной безопасности.
6. Процедурный уровень обеспечения информационной безопасности.
7. Искусственный интеллект в информационной безопасности.
8. Data mining и Text mining как инструменты обеспечения информационной безопасности.
9. Анализ тональности текста.
10. Латентное размещение Дирихле (LDA).
11. Коррелированное тематическое моделирование (CTM).
12. Латентно-семантический анализ (LSA).

Критерии оценивания по зачету:

«зачтено»: студент владеет теоретическими знаниями по данному разделу, допускает незначительные ошибки; студент умеет правильно объяснять теоретический материал, иллюстрируя его примерами различных социальных ситуаций из жизни коллектива и / или организации.

«не зачтено»: материал не усвоен или усвоен частично, студент имеет довольно ограниченный объем знаний программного теоретического материала.

Оценочные средства для инвалидов и лиц с ограниченными возможностями здоровья выбираются с учетом их индивидуальных психофизических особенностей.

- при необходимости инвалидам и лицам с ограниченными возможностями здоровья предоставляется дополнительное время для подготовки ответа на экзамене;
- при проведении процедуры оценивания результатов обучения инвалидов и лиц с ограниченными возможностями здоровья предусматривается использование технических средств, необходимых им в связи с их индивидуальными особенностями;
- при необходимости для обучающихся с ограниченными возможностями здоровья и инвалидов процедура оценивания результатов обучения по дисциплине может проводиться в несколько этапов.

Процедура оценивания результатов обучения инвалидов и лиц с ограниченными возможностями здоровья по дисциплине (модулю) предусматривает предоставление информации в формах, адаптированных к ограничениям их здоровья и восприятия информации:

Для лиц с нарушениями зрения:
- в печатной форме увеличенным шрифтом,
- в форме электронного документа.

Для лиц с нарушениями слуха:
- в печатной форме,
- в форме электронного документа.

Для лиц с нарушениями опорно-двигательного аппарата:
- в печатной форме,
- в форме электронного документа.

Данный перечень может быть конкретизирован в зависимости от контингента обучающихся.

5. Перечень основной и дополнительной учебной литературы, необходимой для освоения дисциплины (модуля).

5.1 Основная литература:

1. Рунаев Т.А. Интеллектуальный анализ текста в социальных науках : учебное пособие / Т.А. Рунаев; Министерство науки и высшего образования Российской Федерации, Кубанский государственный университет. - Краснодар : Кубанский государственный университет, 2024. - 127 с. : ил. - Библиогр.: с. 125. - ISBN 978-5-8209-2404-0. – Режим доступа: http://212.192.134.46/MegaPro/Web/SearchResult/ToPage/1.
2. Суворова, Г. М. Информационная безопасность : учебное пособие для вузов / Г. М. Суворова. — 2-е изд., перераб. и доп. — Москва : Издательство Юрайт,

2024. — 277 с. — (Высшее образование). — ISBN 978-5-534-16450-3. — Текст : электронный // Образовательная платформа Юрайт [сайт]. — URL: https://urait.ru/bcode/544029.
3. Козырь, Н. С. Гуманитарные аспекты информационной безопасности : учебное пособие для вузов / Н. С. Козырь, Н. В. Седых. — Москва : Издательство Юрайт, 2024. — 170 с. — (Высшее образование). — ISBN 978-5-534-17153-2. — Текст : электронный // Образовательная платформа Юрайт [сайт]. — URL: https://urait.ru/bcode/544965
4. Воронов, М. В. Системы искусственного интеллекта : учебник и практикум для вузов / М. В. Воронов, В. И. Пименов, И. А. Небаев. — 2-е изд., перераб. и доп. — Москва : Издательство Юрайт, 2024. — 268 с. — (Высшее образование). — ISBN 978-5-534-17032-0. — Текст : электронный // Образовательная платформа Юрайт [сайт]. — URL: https://urait.ru/bcode/544161

5.2 Дополнительная литература:

1. Основы искусственного интеллекта : учебное пособие / Е.В. Боровская, Н.А. Давыдова. 4-е изд.,электрон. – М. : Лаборатория знаний, 2020. – 130 с.
2. Практики анализа качественных данных в социальных науках: учебное пособие. – Москва: Изд. дом Высшей школы экономики, 2023. – 383 с. – ISBN: 978-5-7598-2542-5.
3. Маккинни У. Python и анализ данных: Первичная обработка данных с применением pandas, NumPy и Jupiter / пер. с англ. А. А. Слинкина. 3-е изд. – М.: МК Пресс, 2023. – 536 с.
4. Храмов Д.А. Сбор данных в Интернете на языке R. – Москва: ДМК Пресс, 2017. – 280 с. – ISBN: 978-5-97060-459-5.
5. Уикэм Х., Гроулмунд Г. Язык R в задачах науки о данных: импорт, подготовка, обработка, визуализация и моделирование данных. – Санкт-Метербург: ООО «Диалектика», 2018. – 592 с. – ISBN: 978-5-9909446-8-8.
6. Kwartler T. Text Mining in Practice with R. – Hoboken: John Wiley & Sons, 2017. – 307 p. – ISBN: 9781119282082.
7. Silge J., Robinson D. Text mining with R. A Tidy Approach. Sebastopol: O'Reilly Media, 2017. – 184 p. – 978-1-491-98165-8.
8. Wiedemann G. Text Mining for Qualitative Data Analysis in the Social Sciences. A Study on Democratic Discourse in Germany. Wiesbaden: Springer, 2016. – 305 p. – ISBN 978-3-658-15308-3.

8.3 Периодические издания:

1) Вестник СПбГУ.Серия: Психология, социология, педагогика
2) Вестник МГУ.Серия: Социология и политология
3) Журнал практического психолога
4) Журналист. Социальные коммуникации
5) Общественные науки и современность
6) Социально-гуманитарные знания
7) СОЦИС / Социологические исследования

6 Перечень ресурсов информационно-телекоммуникационной сети «интернет», необходимых для освоения дисциплины (модуля).

http://lib.socio.msu.ru/l/library - Электронная библиотека социологического факультета МГУ имени М.В. Ломоносова

http://window.edu.ru/window_catalog - Единое окно доступа к образовательным ресурсам

http://www.hh.ru - Хэд Хантер

http://www.isras.ru/ - Институт социологии РАН.

http://www.i-u.ru/biblio - Русский гуманитарный интернет-университет http://www.job.ru - Джоб ру

http://www.kadrovichka.ru - Кадровичка

www.ecsocman.edu.ru - Федеральный образовательный портал по социологии, экономике и менеджменту

www.soc.pu.ru - электронный ресурс социологического факультета Санкт- Петербургского государственного университета

www.socionet.ru - портал по общественным наукам

www.wciom.ru -официальный сайт ВЦИОМ

7. Методические указания для обучающихся по освоению дисциплины (модуля). Рекомендации для самостоятельной работы.

Подготовку к *практическим занятиям* рекомендуется осуществлять по следующему алгоритму: работа с планами семинарских занятий. При подготовке к семинарскому занятию необходимо найти ответы на поставленные вопросы. Рекомендуется делать конспекты в форме тезисов на каждый вопрос.

Для более глубокого понимания и лучшего усвоения экономических категорий и терминов рекомендуется обращаться к основной и дополнительной литературе, работать с информационными ресурсами, справочными материалами и периодическими изданиями. Целесообразно вести собственный словарь терминов и использовать его для повторения.

После изучения материала необходимо построить логическую схему знаний, сформулировать вопросы по тем моментам, которые вызвали затруднения, с целью последующего их вынесения на семинарское занятие для обсуждения.

Важным видом работы студентов при изучении дисциплины является *самостоятельная работа*. Самостоятельная работа должна носить творческий и планомерный характер. В процессе организации самостоятельной работы большое значение имеют консультации преподавателя. Они могут быть как индивидуальными, так и в составе учебной группы.

В освоении дисциплины инвалидами и лицами с ограниченными возможностями здоровья большое значение имеет индивидуальная учебная работа (консультации) - дополнительное разъяснение учебного материала. Индивидуальные консультации по предмету являются важным фактором, способствующим индивидуализации обучения и установлению воспитательного контакта между преподавателем и обучающимся инвалидом или лицом с ограниченными возможностями здоровья.

8. Перечень информационных технологий, используемых при осуществлении образовательного процесса по дисциплине (модулю).

8.1 *Перечень информационных технологий.*

- Использование электронных презентаций при проведении практических занятий.

8.2 *Перечень необходимого программного обеспечения.*

При проведении занятий используется пакет PowerPoint Microsoft Office, ОС Microsoft Windows 10, RStidio, PyCharm.

8.3 *Перечень информационных справочных систем:*

1. Справочно-правовая система «Консультант Плюс» (http://www.consultant.ru)
2. Электронная библиотечная система eLIBRARY.RU (http://www.elibrary.ru)
3. Электронная библиотечная система "Университетская библиотека ONLINE" (www.biblioclub.ru)
4. Электронная библиотечная система издательства "Лань" (http://e.lanbook.com/)
5. Электронная библиотечная система "Юрайт" (http://www.biblio-online.ru)
6. Электронная библиотека "Издательского дома "Гребенников" (www.grebennikon.ru)

9. Материально-техническая база, необходимая для осуществления образовательного процесса по дисциплине (модулю).

№	Вид работ	Материально-техническое обеспечение дисциплины (модуля) и оснащенность

1.	Семинарские занятия	Аудитория, оснащенная презентационной техникой (проектор, экран, компьютер/ноутбук) и соответствующим программным обеспечением (ПО).
2.	Лекционные занятия	Аудитория 244, 246, 249, 250, 258.
3.	Текущий контроль, промежуточная аттестация	Аудитория 244, 246, 249, 250, 258.
4.	Самостоятельная работа	Кабинет для самостоятельной работы, оснащенный компьютерной техникой с возможностью подключения к сети «Интернет», обеспеченный доступом в электронную информационно-образовательную среду университета (библиотека).