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
«02» июня 2026 г.

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ (МОДУЛЯ)

Б1.В.ДВ.04.01 ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ

(код и наименование дисциплины в соответствии с учебным планом)

Направление подготовки/специальность 39.04.01 Социология
(код и наименование направления подготовки/специальности)

Направленность (профиль) / специализация
Социология риска и безопасности
(наименование направленности (профиля) / специализации)

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

Квалификация магистр

Краснодар 2026

Рабочая программа дисциплины Б1.В.ДВ.04.01 Информационная безопасность составлена в соответствии с федеральным государственным образовательным стандартом высшего образования (ФГОС ВО) по направлению подготовки / специальности 39.04.01 Социология

код и наименование направления подготовки

Программу составил(и):

А.Ю. Рожков, профессор кафедры социологии, д-р ист. наук, профессор

И.О. Фамилия, должность, ученая степень, ученое звание — подпись

Рабочая программа дисциплины Б1.В.ДВ.04.01 Информационная безопасность утверждена на заседании кафедры (разработчика) социологии
протокол № 8 «14» апреля 2026 г.
И.о. заведующего кафедрой (разработчика) Т.А. Хагуров

фамилия, инициалы — подпись

Утверждена на заседании учебно-методической комиссии факультета истории, социологии и международных отношений
протокол № 5 «19» мая 2026 г.
Председатель УМК факультета Э.Г. Вартаньян

фамилия, инициалы — подпись

Рецензенты:

Касьянов В.В., декан факультета журналистики, зав. кафедрой истории России ФГБОУ ВО «КубГУ», доктор исторических наук, доктор социологических наук, профессор

Скворцов И.П., профессор кафедры военно-политической работы Краснодарского ВВКУ им. генерала армии С.М. Штеменко, доктор философских наук, профессор

1 Цели и задачи изучения дисциплины

1.1 Цель освоения дисциплины

Формирование у обучающихся системы представлений о разных подходах и возможностях изучения и обоснования специальной социологической теории в определении системы обеспечения информационной безопасности и ее технологий.

1.2 Задачи дисциплины

- обосновать обучающимся необходимость защитных функций общества в целях достижения социальной эффективности механизмов социальной адаптации и устойчивого развития постиндустриального общества с учетом обеспечения надлежащих общественных интересов в информационной сфере;
- выявить состояние информационной безопасности и определить основные формы и тенденции ее развития, показать специфику, роль и социальные последствия, влияющие на характер и коррекцию обеспечения информационной безопасности на российском информационном пространстве;
- сформировать у обучающихся систему знаний об основных теоретических подходах и понятиях в области функционирования системы информационной безопасности в рамках существующего общества и на этой основе сформулировать условия социальной эффективности информационной безопасности в российском социуме;
- выработать у обучающихся целостное представление о разных аспектах функционирования системы информационной безопасности как социальной технологии и разнообразии способов их изучения;
- привить обучающимся практические навыки применения разных теоретических подходов к изучению основ информационной безопасности, навыки применения основных технологий обеспечения информационной безопасности в современных российских условиях.

Место дисциплины (модуля) в структуре образовательной программы Дисциплина «Информационная безопасность» относится к дисциплинам (модулям) Блока 1 «Часть, формируемая участниками образовательных отношений» (Дисциплины (модули) по выбору) учебного плана.

1.3 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 *(ПК)*

Код и наименование индикатора	Результаты обучения по дисциплине
ПК-1 **Способен разрабатывать социологическое обеспечение управления рисками при проведении фундаментальных и прикладных социологических исследований**	
ИПК-1.3. Владеет навыками анализа и интерпретации данных фундаментальных и прикладных социологических исследований (*формируется частично*)	- **знает** классические и современные методы проведения фундаментальных и прикладных социологических исследований в области изучения информационной безопасности - **умеет** применять классические и современные методы проведения фундаментальных и прикладных социологических исследований в области изучения информационной безопасности - **владеет** классической и современной методологией фундаментальных и прикладных социологических исследований в области информационной безопасности
ПК-2 **Способен к осуществлению рискологического анализа для разработки предложений по совершенствованию социально-технологических процессов, методов сбора и анализа информации**	
ИПК-2.1. Осуществляет диагностику и типологизацию	- **знает** основы осуществления диагностики и типологизации рисков в разных сферах

рисков в разных сферах общественной жизни (*формируется частично*)	общественной жизни для разработки предложений по совершенствованию социально-технологических процессов, методов сбора и анализа информации в социологическом исследовании в области информационной безопасности; - **умеет** осуществлять диагностику и типологизацию рисков в разных сферах общественной жизни для разработки предложений по совершенствованию социально-технологических процессов, методов сбора и анализа информации в социологическом исследовании в области информационной безопасности; - **владеет** навыками осуществления диагностики и типологизации рисков в разных сферах общественной жизни для разработки предложений по совершенствованию социально-технологических процессов, методов сбора и анализа информации в социологическом исследовании в области информационной безопасности
ИПК-2.2. Оценивает риски принятия управленческих решений на основе результатов прикладных и фундаментальных исследований (*формируется частично*)	- **знает** основы оценивания рисков принятия управленческих решений на основе результатов прикладных и фундаментальных исследований технологий и методов сбора социологической информации в области информационной безопасности; - **умеет** оценивать риски принятия управленческих решений на основе результатов прикладных и фундаментальных исследований и предлагать новые социальные технологии и методы сбора социологической информации в области информационной безопасности; - **владеет** навыками оценки рисков принятия управленческих решений на основе результатов прикладных и фундаментальных исследований для предложения новых технологий и методов сбора социологической информации в области информационной безопасности
ПК-3 **Способен разрабатывать и проектировать программы профилактики и минимизации рисков в масштабах общества, региона, отдельных социальных групп**	
ИПК-3.1. Разрабатывает программы профилактики рисков в различных сферах (*формируется частично*)	- **знает** основы разработки программ профилактики и минимизации рисков в сфере информационной безопасности; - **умеет** разрабатывать программы профилактики и минимизации рисков в сфере информационной безопасности; - **владеет** навыками разработки программы профилактики и минимизации рисков в сфере информационной безопасности
ИПК-3.2. Владеет навыками разработки социологического обеспечения управления рисками в масштабах общества, региона, отдельных социальных групп (*формируется частично*)	- **знает** основы разработки социологического обеспечения управления рисками в масштабах общества, региона, отдельных социальных групп в области информационной безопасности; - **умеет** разрабатывать социологическое обеспечение управления рисками в масштабах общества, региона, отдельных социальных групп в области информационной безопасности; - **владеет** навыками разработки социологического обеспечения управления рисками в масштабах общества, региона, отдельных социальных групп в области информационной безопасности

2. Структура и содержание дисциплины

2.1 Распределение трудоёмкости дисциплины по видам работ

Общая трудоёмкость дисциплины составляет 3 зач. ед. (108 часов), их распределение по видам работ представлено в таблице *(для студентов ЗФО)*

Виды работ		Всего часов	Форма обучения			
			очная		очно-заочная	заочная
						1 семестр (часы)
Контактная работа, в том числе:		**12,2**				**12,2**
Аудиторные занятия (всего):		**12**				**12**
занятия лекционного типа		6				6
лабораторные занятия		-				-
практические занятия		6				6
Иная контактная работа:						
Контроль самостоятельной работы (КСР)		-				-
Промежуточная аттестация (ИКР)		0,2				0,2
Самостоятельная работа, в том числе:		**92**				**92**
Проработка учебного (теоретического) материала		30				30
Выполнение индивидуальных заданий (подготовка сообщений, презентаций)		30				30
Подготовка к текущему контролю		32				32
Контроль:		**3,8**				**3,8**
Подготовка к экзамену						
Общая трудоемкость	**час.**	**108**				**108**
	в том числе контактная работа	**12,2**				**12,2**
	зач. ед.	**3**				**3**

2.2 Структура дисциплины

Распределение видов учебной работы и их трудоемкости по разделам дисциплины.

Разделы (темы) дисциплины, изучаемые в установочную сессию 1 курса *(заочная форма)*

№	Наименование разделов (тем)	Количество часов				
		Всего	Аудиторная работа			Внеаудиторная работа
			Л	ПЗ	ЛР	СРС
1	2	3	4	5	6	7
1.	Теоретические основы информационной безопасности	17	1	1	-	15
2.	Социологическая концептуализация информационной безопасности	19	1	1	-	17
3.	Государственная политика информационной безопасности	-	-	-	-	-
4.	Основные направления обеспечения информационной безопасности общества	-	-	-	-	-
5.	Когнитивная и информационно-психологическая война	-	-	-	-	-
6.	Методы информационно-психологического влияния	-	-	-	-	-
	ИТОГО по разделам дисциплины					
	Контроль самостоятельной работы (КСР)	-	-	-	-	-
	Промежуточная аттестация (ИКР)	-	-	-	-	-
	Реферат	-	-	-	-	-
	Подготовка к текущему контролю	-	-	-	-	-
	Общая трудоемкость по дисциплине	**36**	**2**	**2**	**-**	**32**

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

Распределение видов учебной работы и их трудоемкости по разделам дисциплины.
Разделы (темы) дисциплины, изучаемые в зимнюю сессию 1 курса *(заочная форма)*

№	Наименование разделов (тем)	Количество часов				
		Всего	Аудиторная работа			Внеаудиторная работа
			Л	ПЗ	ЛР	СРС
1	2	3	4	5	6	7
1.	Теоретические основы информационной безопасности	-	-	-	-	-
2.	Социологическая концептуализация информационной безопасности	-	-	-	-	-
3.	Государственная политика информационной безопасности	17	1	1	-	15
4.	Основные направления обеспечения информационной безопасности общества	17	1	1	-	15
5.	Когнитивная и информационно-психологическая война	17	1	1	-	15
6.	Методы информационно-психологического влияния	17	1	1	-	15
	ИТОГО по разделам дисциплины					
	Контроль самостоятельной работы (КСР)	-	-	-	-	-
	Промежуточная аттестация (ИКР)	0,2	-	-	-	-
	Реферат	-	-	-	-	
	Подготовка к текущему контролю	-	-	-	-	
	Общая трудоемкость по дисциплине	**68**	**4**	**4**	**-**	**60**

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

2.3 Содержание разделов (тем) дисциплины

2.3.1 Занятия лекционного типа

№	Наименование раздела (темы)	Содержание раздела (темы)	Форма текущего контроля
1	2	3	4
1.	Теоретико-методологические основы информационной безопасности	Понятие информационного общества (Ф. Махлуп, У. Мартин и др.). Л. Тоффлер о знании и информации в постиндустриальном обществе. М. Кастельс о трансформации материальной культуры через работу новой технологической парадигмы, построенной вокруг информационных технологий. К.К. Колин об информации как основном движущем факторе развития самоорганизующихся систем. М. Маклюэн об определении технологиями коммуникации восприятия людьми окружающей действительности как объективной реальности. К. Ясперс о тождестве между общением и коммуникацией, а в самой коммуникации – смысле человеческого существования. М.М. Бахтин об интериндивидуальности и интерсубъективности идеи, живущей в пространстве коммуникации между сознаниями и личностями.	*КО* *К*
2.	Социологическая концептуализация информационной безопасности	Развитие информационных технологий как позитивное явление, положительно влияющее на экономическое и технологическое развитие общества. Разрушение «духовного кода» россиян под влиянием массивного и тотального информационного влияния. Информационные угрозы как источник угроз духовной безопасности общества. Социологическая концептуализация понятия «информационная безопасность» предполагает необходимость выделения условий ее формирования, факторов влияния на ее обеспечение, анализа рисков и угроз, исходящих из формирующегося информационного	*КО* *К*

		пространства, тенденций его развития и формирования понятийного инструментария для работы с данной категорией.	
3.	Государственная политика информационной безопасности	Органы обеспечения информационной безопасности как часть государственной системы информационной безопасности и защиты информации. Государственная система защиты информации включает: органы законодательной, исполнительной и судебной властей; законодательство, регулирующее отношения в области защиты информации и информационных ресурсов; нормативную правовую базу по защите информации; службы (органы) защиты информации предприятий, организаций, учреждений. Основные ведомства, регулирующие отношения в области защиты информации: Межведомственная комиссия по защите государственной тайны; Федеральная служба технического и экспортного контроля (ФСТЭК); Госстандарт России; Федеральная служба безопасности (ФСБ РФ), Служба внешней разведки России (СВР) и Федеральная пограничная служба (ФПС).	*Р* *К*
4.	Основные направления обеспечения информационной безопасности общества	Развитие системы информационной безопасности с учетом качественно новых особенностей и состояния современного российского общества. Развитие общественной системы социальной защиты, основанной на активности граждан, различных социальных групп и всех слоев населения, ее взаимодействие с государственной системой социальной защиты. Информационная политика государства. Взаимодействие социальной безопасности и информационной безопасности. Социальные критерии обеспечения информационной безопасности. Тенденции обеспечения технологической части информационной безопасности. Актуальные проблемы обеспечения психофизической части информационной безопасности.	*КО* *К*
5.	Когнитивная и информационно-психологическая война	Ментальная война – противоборство за социально-культурное пространство, в котором формируется ум и мышление, отсюда исключительное значение истории и образования. Когнитивная война как ситуация военного противостояния, в которой потенциально возможно перепрограммирование сознания с использованием современных технологий для навязывания противнику своей воли без обращения к средствам традиционной кинетической войны (физического воздействия) или их использованием в минимальной степени. Когнитивная война рассматривает психофизические аспекты восприятия и познавательной деятельности человека, применяя к ним всю мощь научно-технического и информационного оснащения. Цель – адаптировать или «улучшать» людей с помощью гибридной человеко-системы. Информационная (информационно-психологическая) война – более поверхностная война по передаче информации о себе и противнике, ориентированная на противника и собственное население.	*Р* *К*
6.	Методы информационно-психологического влияния	Размещение на популярных сайтах, видеохостингах и иных сервисах в качестве рекламы в текстовой, фото или видео форме материалов о потерях личного состава и военной техники РФ, зачастую с демонстрацией трупов убитых солдат. Телефонный терроризм (рассылка SMS-сообщений с угрозами, недостоверной информацией, призывами сдаться в плен; телефонные звонки с анонимных номеров с угрозами; телефонные звонки с целью шантажа и/или предложением выкупа пленных военнослужащих и т.д.). Публичное распространение или	*КО* *К*

		угроза распространения персональных данных как военнослужащих, так и гражданских лиц, активно выражающих свою патриотическую позицию. Создание и популяризация различных якобы гуманных программ, с распространением инструкций для сдачи в плен (распространение листовок; использование громкоговорителей на линии боевого соприкосновения с призывом сдаваться; использование средств связи и соцсетей). Взлом радиочастот на линии боевого соприкосновения для трансляции недостоверной информации, а также заявлений и призывов сдаваться в плен. Создание и популяризация экстремистских организаций псевдопатриотического толка в сети Интернет через рекламу, рассылку сообщений, создание и распространение медиаконтента. Операции спецслужб противника, направленные на вовлечение молодежи в незаконную деятельность. Создание и популяризация информационных ресурсов и блогеров якобы из числа местных жителей. Создание фейковых аккаунтов военных корреспондентов, журналистов и общественных деятелей, распространение недостоверной информации. Создание и распространение видеосюжетов от имени рейтинговых СМИ. Информационно-психологические спецоперации, связанные с реальным применением оружия против мирного населения. Подложные сообщения от «очевидцев» про обстрелы населенных пунктов со стороны ВС РФ. Распространение фейковых рейтингов и искаженной статистики о социальных процессах, значимых событиях, политических лидерах.	

2.3.2 Занятия семинарского типа

№	Наименование раздела (темы)	Тематика практических занятий (семинаров)	Форма текущего контроля
1	2	3	4
1.	Теоретико-методологические основы информационной безопасности	Тема: Информационная безопасность как неотъемлемый элемент информационного общества.	*КО* *Д*
2.	Социологическая концептуализация информационной безопасности	Тема: Социологический аспект информационной безопасности общества.	*Р* *КО*
3.	Государственная политика информационной безопасности	Тема: Государственная система информационной безопасности и защиты информации.	*Р* *Д*
4.	Основные направления обеспечения информационной безопасности общества	Тема: Социальные критерии обеспечения информационной безопасности.	*П* *Э*
5.	Когнитивная и информационно-психологическая война	Тема: Ментальная, когнитивная и информационная война: общее и особенное.	*П* *ИКЗ*
6.	Методы информационно-психологического влияния	Тема: Критическое мышление и средства массовой дезинформации и коммуникации.	*П* *Т*

Примечание: выступление с докладом (Д), конспектирование (К), выполнение индивидуального контрольного задания (ИКЗ), написание эссе (Э), рефератов (Р), контрольный опрос (КО), отчет с презентацией (П), тестирование (Т).

2.3.3 Лабораторные занятия - не предусмотрены.

2.3.4 Примерная тематика курсовых работ (проектов) - не предусмотрены.

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

№	Вид СРС	Перечень учебно-методического обеспечения дисциплины по выполнению самостоятельной работы
1	2	3
1	самостоятельное изучение теоретического материала; подготовка к зачетам, экзаменам, выполнение домашних заданий	Методические указания по самостоятельной работе студентов, утвержденные кафедрой социология, протокол № 15 от 23 мая 2017 г. Методические материалы по реализации образовательных технологий, утвержденные кафедрой социология, протокол № 10 от 14 февраля 2017 г.
2	выполнение и оформление докладов, рефератов, эссе	Методические указания по научно-исследовательской работе студентов (направления подготовки 39.03.01, 39.04.01, 39.06.01 Социология), утвержденные кафедрой социология, протокол № 8 от 10 января 2017 г.
3	подготовка к семинарским (практическим) занятиям	Методические указания по самостоятельной работе студентов, утвержденные кафедрой социология, протокол № 15 от 23 мая 2017 г.
4	самостоятельное решение задач, обзор печати	Методические указания по самостоятельной работе студентов, утвержденные кафедрой социология, протокол № 15 от 23 мая 2017 г.
5	самообучение с помощью компьютерных программных средств	Методические материалы по реализации образовательных технологий, утвержденные кафедрой социология, протокол № 10 от 14 февраля 2017 г.
6	текущий самоконтроль усвоения материала	Методические материалы по реализации образовательных технологий, утвержденные кафедрой социология, протокол № 10 от 14 февраля 2017 г.

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,
- в форме аудиофайла,
- в печатной форме на языке Брайля.

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,
- в форме аудиофайла.

Данный перечень может быть конкретизирован в зависимости от контингента обучающихся.

3. Образовательные технологии

Активные и интерактивные формы проведения семинарских и практических занятий - семинары в диалоговом режиме, групповые дискуссии, метод малых групп, работа в команде (при проведении практических занятий), разбор практических задач и кейсов.

Выдача индивидуальных контрольных заданий, включающих самостоятельную отработку теоретической литературы (конспектирование, рефлексию, развернутые ответы на проблемные постановочные вопросы), написание эссе, развернутые ответы на

неформализованную анкету (социологическая биография пользователя информации).

Сравнительные обсуждения личных впечатлений и практик обучающихся при воздействии со стороны пропаганды противника, с учетом локуса их проживания – деревня/малый город; большой город; город на Кубани/города в других регионах России.

Выполнение групповых практических заданий (изучение на конкретных примерах оборонительных и наступательных информационных операций, фейков и антифейков) с последующим отчетом в виде мультимедийной презентации.

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 доклада-презентации по проблемным вопросам, разноуровневых заданий и промежуточной аттестации в форме вопросов и заданий к зачету.

Структура оценочных средств для текущей и промежуточной аттестации

№ п/п	Код и наименование индикатора	Результаты обучения	Наименование оценочного средства	
			Текущий контроль	Промежуточная аттестация
1	ИПК-1.3. Владеет навыками анализа и интерпретации данных фундаментальных и прикладных социологических исследований (*формируется частично*)	- знает классические и современные методы проведения фундаментальных и прикладных социологических исследований в области изучения информационной безопасности - умеет применять классические и современные методы проведения фундаментальных и прикладных социологических исследований в области изучения информационной безопасности - владеет классической и современной методологией фундаментальных и прикладных социологических исследований в области информационной безопасности	*Рефераты, доклады и эссе*	*Вопрос на зачете 1-8*
2	ИПК-2.1. Осуществляет диагностику и типологизацию рисков в разных сферах общественной жизни (*формируется частично*)	- знает основы осуществления диагностики и типологизации рисков в разных сферах общественной жизни для разработки предложений по совершенствованию социально-технологических процессов, методов сбора и анализа информации в социологическом исследовании в области информационной безопасности; - умеет осуществлять диагностику и типологизацию рисков в разных сферах общественной жизни для разработки предложений по	*Индивидуальные контрольные задания* *Рефераты, доклады и эссе* *Тест*	*Вопрос на зачете 9-15*

		совершенствованию социально-технологических процессов, методов сбора и анализа информации в социологическом исследовании в области информационной безопасности; - владеет навыками осуществления диагностики и типологизации рисков в разных сферах общественной жизни для разработки предложений по совершенствованию социально-технологических процессов, методов сбора и анализа информации в социологическом исследовании в области информационной безопасности		
3	ИПК-2.2. Оценивает риски принятия управленческих решений на основе результатов прикладных и фундаментальных исследований (*формируется частично*)	- знает основы оценивания рисков принятия управленческих решений на основе результатов прикладных и фундаментальных исследований технологий и методов сбора социологической информации в области информационной безопасности; - умеет оценивать риски принятия управленческих решений на основе результатов прикладных и фундаментальных исследований и предлагать новые социальные технологии и методы сбора социологической информации в области информационной безопасности; - владеет навыками оценки рисков принятия управленческих решений на основе результатов прикладных и фундаментальных исследований для предложения новых технологий и методов сбора социологической информации в области информационной безопасности	*Индивидуальные и групповые контрольные задания* *Рефераты, доклады и эссе* *Тест*	*Вопрос на зачете 16-20*
4	ИПК-3.1. Разрабатывает программы профилактики рисков в различных сферах (*формируется частично*)	- знает основные методы проведения социологических и маркетинговых исследований в области изучения городских сообществ; - способен выделить социальные явления и процессы, которые можно изучать с позиции анализа городских сообществ;	*Рефераты, доклады и эссе*	*Вопрос на зачете 21-25*
5	ИПК-3.2. Владеет навыками разработки социологического	- знает основы разработки социологического обеспечения управления рисками в масштабах общества, региона,	*Индивидуальные и групповые контрольные задания*	*Вопрос на зачете 26-30*

	обеспечения управления рисками в масштабах общества, региона, отдельных социальных групп (*формируется частично*)	отдельных социальных групп в области информационной безопасности; - умеет разрабатывать социологическое обеспечение управления рисками в масштабах общества, региона, отдельных социальных групп в области информационной безопасности; - владеет навыками разработки социологического обеспечения управления рисками в масштабах общества, региона, отдельных социальных групп в области информационной безопасности	*Рефераты, доклады и эссе* *Тест*	

Типовые контрольные задания или иные материалы, необходимые для оценки знаний, умений, навыков и (или) опыта деятельности, характеризующих этапы формирования компетенций в процессе освоения образовательной программы

Примерные вопросы индивидуального контрольного задания:

1. Какие имеются теоретические основания для тезиса: «Всеобщая вера в революцию есть уже начало революции» (В.И. Ленин). Что означает этот тезис в информационном противоборстве?
2. Приведите примеры технологии расширения рамок допустимого («окна Овертона»). Ответ обоснуйте.
3. Какие манипулятивные задачи решаются с помощью технологии навязывания коллективного мнения? Разберите подробно два кейса: психологические эксперименты С. Аша и С. Московичи. Что в них общего и в чем они различаются?
4. Может ли быть эффективной технология средового влияния на массовое сознание? Разберите подробно технологию Э. Ноэль-Нойман «спираль молчания». Как влияют противоречащие ценностные позиции в различных средах на мнение индивида?
5. Напишите эссе на тему: «Технологии символической маркировки как средство манипуляции массовым сознанием».

Примерные темы докладов (рефератов):

1. Социологическая диагностика национальной аудитории СМК.
2. Национально-самобытная специфика региональных аудиторий СМК.
3. Российское медиапространство как объект информационного воздействия.
4. Западные научные теории как инструмент идеологического прикрытия когнитивной войны.
5. Феномен сетевых войн.
6. Войны памяти как войны когнитивных матриц.
7. Неолиберальные мифы как ментальное оружие.
8. Риски и угрозы развития информационных технологий.
9. Искусственный интеллект в перспективе когнитивных трансформаций.
10. Киборгизация человека и утрата его духовных качеств как результат трансгуманизма.

Примерные темы эссе:

1. Влияние процессов информатизации общества на составляющие национальной безопасности и их содержание.
2. Информационные операции и кибервойна.
3. Информационная война и коммуникации.
4. Современная практика информационных операций.

5. Эволюция информационных операций.
6. Фейки и борьба с ними.
7. Система противодействия информационным операциям.
8. Основные каналы информационного воздействия.
9. Дискредитация научного мировоззрения как технология обмана.
10. Как создать управляемый хаос как оружие?
11. Мемы украинского неонацизма.
12. Украинские учебники по истории как информационно-психологическое оружие.
13. Антироссийские исторические мифы как матрица цивилизационной войны.
14. Критическое мышление и средства массовой дезинформации и коммуникации.
15. Как воздействовать на русский культурный код?

Примерные вопросы теста:

Правильный вариант ответа отмечен знаком +

1) К правовым методам, обеспечивающим информационную безопасность, относятся:

- Разработка аппаратных средств обеспечения правовых данных
- Разработка и установка во всех компьютерных правовых сетях журналов учета действий
+ Разработка и конкретизация правовых нормативных актов обеспечения безопасности

2) Основными источниками угроз информационной безопасности являются:

- Хищение жестких дисков, подключение к сети, инсайдерство
+ Перехват данных, хищение данных, изменение архитектуры системы
- Хищение данных, подкуп системных администраторов, нарушение регламента работы

3) Виды информационной безопасности:

+ Персональная, корпоративная, государственная
- Клиентская, серверная, сетевая
- Локальная, глобальная, смешанная

4) Основные объекты информационной безопасности:

+ Компьютерные сети, базы данных
- Информационные системы, психологическое состояние пользователей
- Бизнес-ориентированные, коммерческие системы

5) Основными рисками информационной безопасности являются:

- Искажение, уменьшение объема, перекодировка информации
- Техническое вмешательство, выведение из строя оборудования сети
+ Потеря, искажение, утечка информации

6) Основными субъектами информационной безопасности являются:

- руководители, менеджеры, администраторы компаний
+ органы права, государства, бизнеса
- сетевые базы данных, фаерволлы

7) Принципом информационной безопасности является принцип недопущения:

+ Неоправданных ограничений при работе в сети (системе)
- Рисков безопасности сети, системы
- Презумпции секретности

8) Принципом политики информационной безопасности является принцип:

+ Разделения доступа (обязанностей, привилегий) клиентам сети (системы)
- Одноуровневой защиты сети, системы
- Совместимых, однотипных программно-технических средств сети, системы.

Примерное групповое контрольное задание на практическое занятие

Цель: организовать противодействие фейковым новостям.

Содержание задания:

Создать рабочую группу, способную сбивать фейки «на взлете» в составе лидера, коммуникатора, аналитика, технолога и ньюсмейкера. Для выполнения задания использовать авторскую методику А.В. Манойло и В.И. Теличко с алгоритмом по распознаванию и отражению фейка:

1) выявить и распознать фейк;
2) осуществить первичный перехват информационной повестки у фейка (разоблачение);
3) создать вирусный антифейк, способный перехватить повестку и вбросить его в информационное пространство;
4) запустить встречную информационную волну, способную сбить фейк «на взлете»;
5) вбросить поддерживающие волну антифейки и иной вирусный контент;
6) провести оперативную социологию.

Подготовить подробный отчет о проделанной работе с мультимедийной презентацией на аудиторном занятии.

Зачетно-экзаменационные материалы для промежуточной аттестации (зачет)

Вопросы для подготовки к зачету

1. Основные тенденции развития информатизации в России.
2. Основные понятия информационной безопасности общества.
3. Информационная безопасность в цифровой экономике.
4. Социологическая информация как объект безопасности.
5. Система защиты информации и ее структура.
6. Информационные угрозы, их виды и причины возникновения.
7. Информационные угрозы для государства.
8. Информационные угрозы для компании.
9. Информационные угрозы для личности (физического лица).
10. Действия и события, нарушающие информационную безопасность.
11. Способы воздействия информационных угроз на объекты.
12. Внешние и внутренние субъекты информационных угроз.
13. Государственное регулирование информационной безопасности.
14. Деятельность международных организаций в сфере информационной безопасности.
15. Нормативно-правовые аспекты в области информационной безопасности в России.
16. Доктрина информационной безопасности Российской Федерации.
17. Федеральные законы по ИБ в РФ.
18. Политика безопасности и ее принципы.
19. Организационное обеспечение ИБ.
20. Обеспечение информационной безопасности: содержание и структура понятия.
21. Национальные интересы в информационной сфере.
22. Источники и содержание угроз в информационной сфере.
23. Соотношение понятий «информационная безопасность» и «национальная
24. безопасность».
25. Система обеспечения информационной безопасности в Российской Федерации.
26. Понятие и виды информационной войны.
27. Информационное оружие и его классификация.
28. Цели информационной войны, ее составные части и средства ведения.
29. Уровни ведения информационной войны. Информационно-психологические операции.
30. Основные положения государственной информационной политики Российской Федерации.

Критерии оценки ответа студента на зачете:

7) оценка «зачтено» выставляется студенту, если изложено развернутое понимание вопроса и дан исчерпывающий ответ; содержание раскрыто полно, профессионально, грамотно; продемонстрировано глубокое знание программного материала, а также основного содержания и новаций курса по сравнению с учебной литературой; ответ свидетельствует о способности самостоятельно критически оценивать основные положения учебного курса; допускаются малосущественные ошибки и пропуски;
8) оценка «не зачтено» выставляется студенту, если материал излагается непоследовательно, сбивчиво, не представляет определенной системы знаний по учебному курсу; студент демонстрирует существенные пробелы в знании основного материала по программе и допускает принципиальные ошибки при изложении материала; неуверенно, с большими затруднениями выполняет практические задания.

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

5.1 Учебная литература

1. Кравченко, С. А. Социология риска и безопасности : учебник и практикум для вузов / С. А. Кравченко. — Москва : Издательство Юрайт, 2026. — 272 с. — (Высшее образование). — ISBN 978-5-534-16508-1. — Текст : электронный // Образовательная платформа Юрайт [сайт]. — URL: https://urait.ru/bcode/583863 (дата обращения: 22.06.2026).
2. Чернова, Е. В. Информационная безопасность человека : учебник для вузов / Е. В. Чернова. — 3-е изд., перераб. и доп. — Москва : Издательство Юрайт, 2026. — 327 с. — (Высшее образование). — ISBN 978-5-534-16772-6. — Текст : электронный // Образовательная платформа Юрайт [сайт]. — URL: https://urait.ru/bcode/587699 (дата обращения: 22.06.2026).
3. Чернова, Е. В. Информационная безопасность человека : учебник для вузов / Е. В. Чернова. — 3-е изд., перераб. и доп. — Москва : Издательство Юрайт, 2026. — 327 с. — (Высшее образование). — ISBN 978-5-534-16772-6. — Текст : электронный // Образовательная платформа Юрайт [сайт]. — URL: https://urait.ru/bcode/587699 (дата обращения: 22.06.2026).
4. Козырь, Н. С. Анализ и оценка рисков информационной безопасности : учебник для вузов / Н. С. Козырь, В. Н. Хализев. — Москва : Издательство Юрайт, 2026. — 157 с. — (Высшее образование). — ISBN 978-5-534-17866-1. — Текст : электронный // Образовательная платформа Юрайт [сайт]. — URL: https://urait.ru/bcode/590420 (дата обращения: 22.06.2026).
5. Зенков, А. В. Информационная безопасность и защита информации : учебник для вузов / А. В. Зенков. — 2-е изд., перераб. и доп. — Москва : Издательство Юрайт, 2026. — 107 с. — (Высшее образование). — ISBN 978-5-534-16388-9. — Текст : электронный // Образовательная платформа Юрайт [сайт]. — URL: https://urait.ru/bcode/588741 (дата обращения: 22.06.2026).
6. Ковалев, Д. В. Информационная безопасность : учебное пособие : [16+] / Д. В. Ковалев, Е. А. Богданова ; Южный федеральный университет. – Ростов-на-Дону : Южный федеральный университет, 2016. – 74 с. : схем., табл., ил. – Режим доступа: по подписке. – URL: https://biblioclub.ru/index.php?page=book&id=493175 (дата обращения: 22.06.2026). – Библиогр. в кн. – ISBN 978-5-9275-2364-1. – Текст : электронный.
7. Суворова, Г. М. Информационная безопасность : учебник для вузов / Г. М. Суворова. — 2-е изд., перераб. и доп. — Москва : Издательство Юрайт, 2026. — 277 с. — (Высшее образование). — ISBN 978-5-534-16450-3. — Текст : электронный // Образовательная платформа Юрайт [сайт]. — URL: https://urait.ru/bcode/588515 (дата обращения: 22.06.2026).
8. Щербак, А. В. Информационная безопасность : учебник для вузов / А. В. Щербак. — 2-е изд. — Москва : Издательство Юрайт, 2026. — 252 с. — (Высшее образование). — ISBN 978-5-9916-4299-6. — Текст : электронный // Образовательная платформа Юрайт [сайт]. — URL: https://urait.ru/bcode/589902 (дата обращения: 22.06.2026).

5.2 Периодическая литература

Журнал «Вестник МГУ». Сер. Социология и политология http://www.shpl.ru/docdelive/couteus/hist/v_mgu_s199902.htm/

Журнал «Вопросы управления» http://vestnik.uapa.ru/ru/about/

Журнал «Государственное и муниципальное управление. Ученые записки СКАГС» http://upravlenie.uriu.ranepa.ru/

Журнал «Общественные науки и современность» http://ecsocman.hse.ru/ons/

Журнал социологии и социальной антропологии http://www.jourssa.ru

Журнал «Социология: 4М (методология, методика, математическое моделирование)» http://www.isras.ru/4M.html

Журнал «Социология власти» http://www.rags.ru/sc/subscrib.htm

Журнал «Социологический журнал» http://www.socjournal.ru

Журнал «Социологическое обозрение» http://sociologica.hse.ru

Журнал «Социология управления и государственной службы» http://pnu.edu.ru/vestnik/pub/categories/93/

Журнал «Социум и власть» http://siv74.ru/index.php

Журнал исследований социальной политики http://ecsocman.hse.ru/mags/jsps

Журнал «Информация и безопасность» https://cchgeu.ru/science/nauchnye-izdaniya/nauchnyy-zhurnal-informatsiya-i-bezopasnost/

Журнал «Информационная безопасность» https://cchgeu.ru/science/nauchnye-izdaniya/nauchnyy-zhurnal-informatsiya-i-bezopasnost/

Журнал «Вестник УрФО. Безопасность в информационной среде» https://www.info-secur.ru/old/

5.3 Интернет-ресурсы, в том числе современные профессиональные базы данных и информационные справочные системы Электронно-библиотечные системы (ЭБС):

ЭБС «ЮРАЙТ» https://urait.ru/

ЭБС «УНИВЕРСИТЕТСКАЯ БИБЛИОТЕКА ОНЛАЙН» www.biblioclub.ru

ЭБС «BOOK.ru» https://www.book.ru

ЭБС «ZNANIUM.COM» www.znanium.com

ЭБС «ЛАНЬ» https://e.lanbook.com

Профессиональные базы данных:

Web of Science (WoS) http://webofscience.com/

Scopus http://www.scopus.com/

ScienceDirect www.sciencedirect.com

Научная электронная библиотека (НЭБ) http://www.elibrary.ru/

Полнотекстовые архивы ведущих западных научных журналов на Российской платформе научных журналов НЭИКОН http://archive.neicon.ru

Национальная электронная библиотека (доступ к Электронной библиотеке диссертаций Российской государственной библиотеки (РГБ) https://rusneb.ru/

Президентская библиотека им. Б.Н. Ельцина https://www.prlib.ru/

Электронная коллекция Оксфордского Российского Фонда
https://ebookcentral.proquest.com/lib/kubanstate/home.action

Springer Journals https://link.springer.com/

"Лекториум ТВ" http://www.lektorium.tv/

Университетская информационная система РОССИЯ http://uisrussia.msu.ru

Альманах «Мастер». Сборник статей по социологии, психологии, экономике http://rpg.nsk.ru/texts/rpg/lections/almanax/oglav.htm

Всероссийский Центр Изучения Общественного мнения [Официальный сайт] http://www.wciom.ru

Группа «Мониторинг» [Официальный сайт] http://www.monitoring.ru
Группа ЦИРКОН [Официальный сайт] http://www.zircon.ru
Институт независимых социологических исследований [Официальный сайт] http://www.indepsocres.spb.ru
Институт социально-политических исследований РАН [Официальный сайт] http://www.ispr.ras.ni/
Институт социологии Российской академии наук http://www.isras.ru
Компания Gallup Media [Официальный сайт] http://www.gallup.ru/
ПостНаука [сайт] https://postnauka.ru/faq/59648
Российское образование, федеральный портал [Официальный сайт] http://www.edu.ru
Российское общество социологов [Официальный сайт] http://www.isras.rssi.ru/ROS_Site.htm
Сервер органов государственной власти [Официальный сайт] РФ http://www.gov.ru/
Фонд «Общественное мнение» [Официальный сайт] http://www.fom.ru
Центр независимых социологических исследований https://cisr.ru/
Центр социально-политического анализа [Официальный сайт] http://www.riisnp.ru/rus/russian/center3.html
Электронная библиотека по социальным и гуманитарным дисциплинам http://www.auditorium.ru

Информационные справочные системы:
Консультант Плюс – справочная правовая система (доступ по локальной сети с компьютеров библиотеки)

Ресурсы свободного доступа:
Полные тексты канадских диссертаций http://www.nlc-bnc.ca/thesescanada/
КиберЛенинка (http://cyberleninka.ru/);
Министерство науки и высшего образования Российской Федерации https://www.minobrnauki.gov.ru/;
Федеральный портал "Российское образование" http://www.edu.ru/;
Информационная система "Единое окно доступа к образовательным ресурсам" http://window.edu.ru/;
Единая коллекция цифровых образовательных ресурсов http://school-collection.edu.ru/ .
Федеральный центр информационно-образовательных ресурсов (http://fcior.edu.ru/);
Проект Государственного института русского языка имени А.С. Пушкина "Образование на русском" https://pushkininstitute.ru/;
Служба тематических толковых словарей http://www.glossary.ru/;
Словари и энциклопедии http://dic.academic.ru/;
Образовательный портал "Учеба" http://www.ucheba.com/;
Законопроект "Об образовании в Российской Федерации". Вопросы и ответы http://xn--273--84d1f.xn--p1ai/voprosy_i_otvety

Собственные электронные образовательные и информационные ресурсы КубГУ:
Среда модульного динамического обучения http://moodle.kubsu.ru
База учебных планов, учебно-методических комплексов, публикаций и конференций http://mschool.kubsu.ru/
Библиотека информационных ресурсов кафедры информационных образовательных технологий http://mschool.kubsu.ru;
Электронный архив документов КубГУ http://docspace.kubsu.ru/

Электронные образовательные ресурсы кафедры информационных систем и технологий в образовании КубГУ и научно-методического журнала "ШКОЛЬНЫЕ ГОДЫ" http://icdau.kubsu.ru/

6. Методические указания для обучающихся по освоению дисциплины (модуля).

Общие рекомендации по самостоятельной работе.

Самостоятельная работа обучаемых проводится для закрепления и углубления полученных знаний, изучения актуальных теоретических и практических проблем социологии города. Студенты обучаются формам и методам доработки теоретического материала, изучения источников вторичных данных, документов органов государственной власти и управления, материалов средств массовой информации.

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.

Содержание самостоятельной работы студента включает: цели самостоятельной работы по разделам (модулям), используемые виды и планируемые результаты. Основными видами самостоятельной работы студента являются:

- изучение теоретического материала;
- самостоятельное изучение отдельных разделов и тем дисциплины;
- работа с учебной и научной литературой;
- выполнение и оформление докладов, рефератов, эссе;
- подготовка к семинарским (практическим) занятиям;
- решение задач, обзор печати;
- текущий самоконтроль усвоения материала;
- самообучение с помощью компьютерных программных средств;
- подготовка к зачетам, экзаменам, выполнение домашних заданий и т.п.

Самостоятельная работа студента с участием преподавателя также включает в себя групповые и индивидуальные консультации.

Подготовку к *практическим и семинарским занятиям* рекомендуется осуществлять по следующему алгоритму:

1. Работа с конспектом лекций по курсу.
2. Работа с планами практических (семинарских) занятий.
3. Работа с рекомендованной учебной литературой.

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.

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. Индивидуальные консультации могут проводиться как в аудиториях университета, так и посредством электронной информационно-образовательной среды организации.

7. Материально-техническое обеспечение по дисциплине (модулю)

По всем видам учебной деятельности в рамках дисциплины используются аудитории, кабинеты и лаборатории, оснащенные необходимым специализированным и лабораторным оборудованием.

№	Вид работ	Материально-техническое обеспечение дисциплины (модуля) и оснащенность
1.	Лекционные занятия	Учебная аудитория для проведения занятий лекционного типа (ауд. 249), ул. Ставропольская 149. 64 посадочных места, 1 мультимедийный проектор, 1 магнитно-меловая доска (зелёная). Учебная аудитория для проведения занятий лекционного типа (ауд. 250), ул. Ставропольская 149. 64 посадочных места, 1 телевизор HDMI, 1 магнитно-меловая доска (зелёная).
2.	Семинарские занятия	Учебная аудитория для проведения занятий семинарского типа (ауд. 256), ул. Ставропольская 149. 20 посадочных мест, 1 телевизор VHS, 1 магнитно-меловая доска (зелёная). Учебная аудитория для проведения занятий семинарского типа (ауд. А210), ул. Ставропольская 149. 36 посадочных мест, 1 магнитно-маркерная доска (белая), 1 меловая доска.
3.	Лабораторные занятия	Не предусмотрены
4.	Курсовое проектирование	Не предусмотрены
5.	Групповые (индивидуальные) консультации	Учебная аудитория для проведения занятий семинарского типа (ауд. 256), ул. Ставропольская 149. 20 посадочных мест, 1 телевизор VHS, 1 магнитно-меловая доска (зелёная). Учебная аудитория для проведения занятий семинарского типа (ауд. А210), ул. Ставропольская 149. 36 посадочных мест, 1 магнитно-маркерная доска (белая), 1 меловая доска.
6.	Текущий контроль, промежуточная аттестация	Учебная аудитория для проведения занятий семинарского типа (ауд. 256), ул. Ставропольская 149. 20 посадочных мест, 1 телевизор VHS, 1 магнитно-меловая доска (зелёная). Учебная аудитория для проведения занятий семинарского типа (ауд. А210), ул. Ставропольская 149. 36 посадочных мест, 1 магнитно-маркерная доска (белая), 1 меловая доска.
7.	Самостоятельная работа	Помещение для самостоятельной работы (ауд. 259), ул. Ставропольская 149. 7 посадочных мест, 1 ПЭВМ.