

Федеральное государственное бюджетное образовательное учреждение
высшего образования
Московский государственный университет имени М.В. Ломоносова
Высшая школа (факультет) телевидения

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ (МОДУЛЯ)
Наименование дисциплины (модуля):

ЦИФРОВАЯ БЕЗОПАСНОСТЬ
Уровень высшего образования:
Бакалавриат

Направление подготовки (специальность):
42.03.04 – «Телевидение»

Форма обучения:
очная

Рабочая программа рассмотрена и одобрена
на заседании Ученого Совета Высшей школы (факультета) телевидения
(протокол №7 от 30.08.2023 г.)

Москва 2023

Рабочая программа дисциплины (модуля) разработана в соответствии с самостоятельно установленным МГУ имени М.В.Ломоносова образовательным стандартом (ОС МГУ) для реализуемых основных профессиональных образовательных программ высшего образования по направлению подготовки 42.03.04 Телевидение (программ бакалавриата), утвержденным приказом ректора МГУ «Об утверждении образовательного стандарта МГУ имени М.В.Ломоносова» Утвержден приказом МГУ от 30 августа 2019 года № 1038 (в редакции приказов МГУ от 11 сентября 2019 года № 1109, от 10 июня 2021 года № 609, от 21 декабря 2021 года № 1404, от 29.05.2023 года № 2).

Год (годы) приема на обучение: 2020, 2021, 2022, 2023.

1. Место дисциплины (модуля) в структуре ОПОП ВО.

Дисциплина «Цифровая безопасность» реализуется в рамках вариативной части программы бакалавриата и является дисциплиной по выбору студента.

В качестве промежуточной аттестации по дисциплине предусмотрен зачет в 7-м семестре и зачет с оценкой в 8 семестре у обучающихся в очной форме обучения.

Итоговая оценка уровня сформированности компетенций ПК-1; ПК-4; ПК-6; ПК-7 определяется в период государственной итоговой аттестации.

2. Входные требования для освоения дисциплины (модуля), предварительные условия (если есть).

Дисциплина «Цифровая безопасность» направлена на формирование и развитие у студентов знаний и навыков в области безопасности и защиты информации. В рамках курса „Цифровая безопасность” студенты познакомятся со свойствами информации как объекта защиты, узнают закономерности создания защищённых информационных систем, получают информацию о принципах обеспечения информационной безопасности государства, отдельное время уделяется теме информационных войн и информационному противоборству.

В ходе данного курса студенты познакомятся с основными моделями цифровой безопасности, а также узнают о международных стандартах в области информационной безопасности, детально познакомятся с понятиями и терминами, принятыми в сфере как цифровой, так и информационной безопасности.

Цели освоения дисциплины

Дисциплина «Цифровая безопасность» дает студентам необходимые знания в области информационной безопасности, вырабатывает навыки и формирует представления о принципах и механизмах функционирования информации в условиях цифровой безопасности. В ходе изучения дисциплины студенты учатся применять на практике знания о механизмах защиты и проверки информации. В рамках курса студенты получают обширные знания по заявленной дисциплине, которые соотносятся с практическими задачами профессиональной сферы.

Непосредственными целями дисциплины являются:

- ознакомить студентов с основными понятиями и терминами в области цифровой безопасности;
- дать представление о принципах и методах защиты информации разного уровня;
- продемонстрировать на примерах способы эффективного использования защитных систем информации;

Процесс изучения дисциплины направлен на формирование следующих компетенций у студентов:

- овладение технологиями цифровой защиты информации;
- способность организовать процесс создания цифровой защиты информации;
- овладение максимальным количеством категорий защиты информации;
- усвоить понятие цифровой гигиены в медиaprостранстве;
- способность участвовать в создании цифровых защитных систем информации.

В результате освоения дисциплины обучающийся должен

Знать: основные понятия, определения и концепции, связанные с цифровой безопасностью.

Уметь: создать цифровую защиту информации; планировать ход работы над созданием цифровой системы защиты информации; при необходимости работать в команде и распределять обязанности в рамках рабочей группы; использовать современные

технические средства для создания цифровых систем защиты информации; применить полученные знания для самостоятельной работы в области цифровой безопасности.

Владеть: теоретическими знаниями и практическими навыками, необходимыми для работы в области цифровой безопасности; навыками эффективного использования инструментов для защиты информации в киберпространстве; навыками грамотного и продуктивного использования современных средств по защите информации в цифровой среде.

Дисциплина «Цифровая безопасность» относится к курсам по выбору, изучается в 7,8 семестрах на 4 курсе и опирается на теоретические и практические основы ранее пройденных дисциплин: «Теория и практика современной телевизионной журналистики», «Телережиссура», «Телематургия (сценарное дело)», «Операторское дело», «Телевизионный монтаж», «Звукорежиссура» и пр.

3. Результаты обучения по дисциплине (модулю), соотнесенные с требуемыми компетенциями выпускников.

Код и описание компетенции	Планируемые результаты обучения по дисциплине	Код и наименование индикатора достижения общепрофессиональной компетенции
<p>ПК-1 Способен осуществлять авторскую деятельность с учетом специфики телевидения и других экранных масс-медиа и практики современной экранной культуры</p>	<p>Знает: особенности осуществления авторской деятельности с учетом специфики телевидения и других экранных масс-медиа и практики современной экранной культуры.</p>	<p>ПК-1.1. Осуществляет регулярный мониторинг актуальных тем и выявляет существующие проблемы информационной повестки дня</p>
	<p>Умеет: осуществлять авторскую деятельность с учетом специфики телевидения и других экранных масс-медиа и практики современной экранной культуры.</p>	<p>ПК-1.2. Создаёт продуманную сценарную основу телевизионного и мультимедийного продукта с учётом формата и жанровых особенностей</p>
	<p>Владеет: навыками осуществления авторской деятельности с учетом специфики телевидения и других экранных масс-медиа и практики современной экранной культуры.</p>	<p>ПК-1.3. Разрабатывает сложное мультимедийное решение телевизионного и мультимедийного продукта с учётом целевой аудитории</p>
		<p>ПК-1.4. Воплощает авторский и режиссерский замысел аудиовизуальными средствами на основе современных цифровых технологий</p> <p>ПК-1.5. Анализирует</p>

		<p>релевантную информацию из доступных документальных и архивных источников</p> <p>ПК-1.6. Разрабатывает оригинальные творческие концепции с учетом опыта конкурентов</p> <p>ПК-1.7. Готовит телевизионный продукт любого уровня сложности к выпуску в эфир с учетом требований конкретного СМИ или другого медиа</p>
<p>ПК-4 Способен организовывать процесс создания телевизионного и мультимедийного продукта.</p>	<p>Знает: особенности организации процесса создания телевизионного и мультимедийного продукта.</p>	<p>ПК-4.1. Готовит материал для выпуска программы в эфир</p>
	<p>Умеет: организовывать процесс создания телевизионного и мультимедийного продукта.</p>	<p>ПК-4.2. Производит репетирование, съемку программ</p>
	<p>Владеет: навыками особенности организации процесса создания телевизионного и мультимедийного продукта.</p>	<p>ПК-4.3. Обеспечивает производственный процесс создания телевизионного и мультимедийного продукта необходимыми ресурсами</p> <p>ПК-4.4. Организует хозяйственную деятельность по созданию телевизионного и мультимедийного продукта</p> <p>ПК-4.5. Контролирует изготовление исходных материалов телевизионного и мультимедийного продукта</p>
<p>ПК-6 Способен продвигать телевизионный и мультимедийный продукт путем взаимодействия с социальными группами, организациями и персонами с помощью различных каналов коммуникации.</p>	<p>Знает: особенности продвижения телевизионного и мультимедийного продукта путем взаимодействия с социальными группами, организациями и персонами с помощью различных каналов аудиовизуальной коммуникации.</p>	<p>ПК-6.1. Просчитывает финансовую составляющую нового телевизионного и мультимедийного продукта</p>
	<p>Умеет: продвигать телевизионный и мультимедийный продукт путем взаимодействия с социальными группами, организациями и персонами с помощью различных каналов аудиовизуальной коммуникации</p>	<p>ПК-6.2. Организует продвижение готовых телевизионных и мультимедийных продуктов на этапе создания с помощью различных каналов аудиовизуальной коммуникаций</p>

аудиовизуальной коммуникации.	каналов аудиовизуальной коммуникации.	
	Владеет: навыками продвижения телевизионного и мультимедийного продукта путем взаимодействия с социальными группами, организациями и персонami с помощью различных каналов аудиовизуальной коммуникации.	
ПК-7 Способен участвовать в социальной и культурно-просветительской деятельности.	Знает: особенности социальной и культурно-просветительской деятельности.	ПК-7.2. Применяет навыки культурно-просветительского воздействия на аудиторию ПК-7.2. Разрабатывает и реализует социальные и культурно-просветительские телевизионные проекты
	Умеет: участвовать в социальной и культурно-просветительской деятельности.	
	Владеет: навыками работы в социальной и культурно-просветительской деятельности.	

4. Формат обучения – очная форма.

5. Объем дисциплины (модуля) составляет 3 з.е., 108 часа, в том числе 54 академических часов, отведенных на контактную работу обучающихся с преподавателем, 54 академических часа на самостоятельную работу обучающихся.

6. Содержание дисциплины (модуля), структурированное по темам (разделам) с указанием отведенного на них количества академических часов и виды учебных занятий

№ п/п	Раздел Дисциплины	Всего	Виды учебной работы, включая самостоятельную работу студентов и трудоемкость (в часах)			Формы текущего контроля успеваемости (по неделям семестра)
			Лекции	Семинары	Самостоятельная работа студента	
1.	Вводное теоретическое занятие: основные понятия теории цифровой безопасности.	8		4	4	Устный опрос
2.	Информация как объект	8		4	4	Устный опрос

	защиты.					
3.	Угрозы информационной безопасности.	8		4	4	Устный опрос
4.	Основные принципы построения систем защиты информации и правовые понятия в области защиты информации.	8		4	4	Устный опрос
5.	Правовые понятия в области защиты цифровой информации.	8		4	4	Устный опрос
6.	Модели цифровой информационной безопасности	8		4	4	Устный опрос
7.	Обзор международных стандартов цифровой информационной безопасности.	8		4	4	Устный опрос
Зачет						
8.	Информационные войны: методология ведения, цели и задачи.	8		4	4	Устный опрос
9.	Роль СМИ в информационной войне.	8		4	4	Устный опрос
10.	Основные направления в сфере киберпреступлений.	8		4	4	Устный опрос
11.	Социальная инженерия: спам, фишинг, вымогательство.	8		4	4	Устный опрос
12.	Правила гигиены.	8		4	4	Устный опрос
13.	Цифровой след человека в сети	8		4	4	Устный опрос
14.	Техника эффективной коммуникации в цифровом мире.	4		2	2	Устный опрос
Итоговая аттестация: зачет с оценкой						
	Всего:	108		54	54	

Краткое содержание дисциплины (модуля)

№ п/п	Наименование раздела дисциплины	Содержание раздела
1.	Вводное теоретическое занятие: основные понятия теории цифровой безопасности	Основные цели и задачи дисциплины. Особенности работы с группой в течение семестра: построение семинарских занятий и рекомендации по самостоятельной работе студента. Критерии оценки

		промежуточных результатов и оценки финальной работы. Эволюция понятия цифровой безопасности. Предметная область и систематизация основных терминов и концепций в области цифровой безопасности.
2.	Информация как объект защиты.	Понятие об информации как объекте защиты. Особенности объекта защиты. Уровни представления информации. Основные свойства защищаемой информации. Виды и формы предоставляемой информации. Информационные ресурсы. Классификация, структура и шкала ценностей информации.
3.	Угрозы информационной безопасности	Анализ уязвимой системы. Классификация угроз цифровой информационной безопасности. Основные направления и методы реализации угроз. Классификация нарушителей. Оценка уязвимости системы
4.	Основные принципы построения систем защиты цифровой информации.	Возможные системы защиты информации. Концепция комплексной защиты информации. Задачи защиты информации. Средства реализации комплексной защиты информации. Построение систем защиты от угрозы нарушения целостности информации и отказа доступа.
5.	Правовые понятия в области защиты цифровой информации.	Правовой режим информационных ресурсов. Информационная безопасность и ее место в системе национальной безопасности РФ. Основные органы обеспечения информационной безопасности и защиты информации, их функции и задачи, нормативная деятельность.
6.	Модели цифровой информационной безопасности.	Основные цели и задачи создания политики безопасности. Субъектно-объектные разграничения доступа к цифровой информации. Основные аксиомы политик безопасности. Парольные разграничения доступа. Политика и модели мандатного доступа. Теоретико-информационные модели информационной безопасности. Тематическое разграничение доступа к цифровой информации.
7.	Обзор международных стандартов цифровой информационной безопасности.	Роль стандартов информации в целом и цифровой, в частности. Критерии (классы) безопасности компьютерных систем США. Европейские критерии безопасности информационных технологий. Единые мировые критерии безопасности информационных технологий.
8.	Информационные войны: методология ведения, цели и задачи	Определение и основные виды информационных войн. Структура информационной войны. Эволюция понятий и представлений об информационной войне. Информационно-техническая и информационно-психологическая война. Роль периода экспозиции. Основная итерационная система. Механизм коррекции.
9.	Роль СМИ в информационной войне.	Практика организации и проведения информационных операций. Как создаются мифы. Каскады. Выбор объекта (мишени). Какой должна быть информация в

		информационном вбросе, чтобы ей поверили. Операции по легализации вбрасываемой информации.
10.	Основные направления в сфере киберпреступлений.	Как защитить личность в цифровую эпоху. Классификация киберугроз. Общие правила цифровой безопасности. Вредные приложения. Продажа неявного доступа к устройству. Вымогатели. Компьютерный вирус и троянские программы. Дистрибуция программного обеспечения.
11.	Социальная инженерия: спам, фишинг, вымогательство.	Социотехника – набор приёмов психологической манипуляции. Спамы, слежка, фишинг, деньги с неба., платные опросы, конкурсы и выигрыши.
12.	Правила кибергигиены.	Гигиена мобильного счета. Гигиена мобильной связи. Гигиена СМС-общения. Управление паролями. Гигиена электронной почты.
13.	Цифровой след человека в сети	Внешние наблюдатели. Независимые наблюдатели. Технологии глубоких фейков. Социальные сети: угрозы и опасности.
14.	Техника эффективной коммуникации в цифровом мире.	Базовые подходы к расширению коммуникативного ресурса в цифровом мире. Условия для эффективной коммуникации.

7. Фонд оценочных средств (ФОС) для оценивания результатов обучения по дисциплине (модулю)

Рекомендуемые образовательные технологии

Лекции; практические занятия по освоению навыков работы с различными программами по созданию цифровой защиты информации. Самостоятельная работа студентов включает написание реферата и отработка навыков защиты информации в цифровой среде.

Основной способ представления материала дисциплины – семинары и практические занятия. В рамках занятий важное место занимает визуальная демонстрация преподавателем актуального фактического материала.

Типовые контрольные задания или иные материалы для проведения промежуточной аттестации.

Примерный перечень тем для проведения промежуточного контроля

1. Вводное теоретическое занятие: основные понятия теории цифровой безопасности.
2. Информация как объект защиты.
3. Угрозы информационной безопасности.
4. Основные принципы построения систем защиты информации и правовые понятия в области защиты информации.
5. Правовые понятия в области защиты цифровой информации.
6. Модели цифровой информационной безопасности
7. Обзор международных стандартов цифровой информационной безопасности.
8. Информационные войны: методология ведения, цели и задачи.
9. Роль СМИ в информационной войне.
10. Основные направления в сфере киберпреступлений.
11. Социальная инженерия: спам, фишинг, вымогательство.
12. Правила кибергигиены.
13. Цифровой след человека в сети

14.Техника эффективной коммуникации цифровом мире.

ШКАЛА И КРИТЕРИИ ОЦЕНИВАНИЯ результатов обучения (РО) по дисциплине (модулю)				
Оценка	2	3	4	5
РО и соответствующие виды оценочных средств				
Знания (виды оценочных средств: устные и письменные опросы и контрольные работы, тесты, и т.п.)	Отсутствие знаний	Фрагментарные знания	Общие, но не структурированные знания	Сформированные систематические знания
Умения (виды оценочных средств: практические контрольные задания, написание и защита рефератов на заданную тему и т.п.)	Отсутствие умений	В целом успешное, но не систематическое умение	В целом успешное, но содержащее отдельные пробелы умение (допускает неточности неприципиального характера)	Успешное и систематическое умение
Навыки (владения, опыт деятельности) (виды оценочных средств: выполнение и защита курсовой работы, отчет по практике, отчет по НИР и т.п.)	Отсутствие навыков (владений, опыта)	Наличие отдельных навыков (наличие фрагментарного опыта)	В целом, сформированные навыки (владения), но используемые не в активной форме	Сформированные навыки (владения), применяемые при решении задач

Шкала оценивания, в зависимости от уровня сформированности компетенций

Уровень сформированности компетенций

<p>«недостаточный» Компетенции не сформированы.</p> <p>Знания отсутствуют, умения и навыки не сформированы</p>	<p>«пороговый» Компетенции сформированы.</p> <p>Сформированы базовые структуры знаний. Умения фрагментарны и носят репродуктивный характер. Демонстрируется низкий уровень самостоятельности практического навыка.</p>	<p>«продвинутый» Компетенции сформированы.</p> <p>Знания обширные, системные. Умения носят репродуктивный характер применяются к решению типовых заданий. Демонстрируется достаточный уровень самостоятельности устойчивого практического навыка.</p>	<p>«высокий» Компетенции сформированы.</p> <p>Знания твердые, аргументированные, всесторонние. Умения успешно применяются к решению как типовых так и нестандартных творческих заданий. Демонстрируется высокий уровень самостоятельности, высокая адаптивность практического навыка</p>
Описание критериев оценивания			
<p>Студент демонстрирует:</p> <ul style="list-style-type: none"> - существенные пробелы в знаниях учебного материала; - допускаются принципиальные ошибки при ответе на основные вопросы билета, отсутствует знание и понимание основных понятий и категорий; - непонимание сущности дополнительных вопросов в рамках заданий билета; - отсутствие умения выполнять практические задания, предусмотренные программой дисциплины; - отсутствие готовности (способности) к дискуссии и низкую степень контактности. 	<p>Студент демонстрирует:</p> <ul style="list-style-type: none"> - знания теоретического материала; - неполные ответы на основные вопросы, ошибки в ответе, недостаточное понимание сущности излагаемых вопросов; - неуверенные и неточные ответы на дополнительные вопросы. - недостаточное владение литературой, рекомендованной программой дисциплины; - умение, без грубых ошибок, решать практические задания, которые следует выполнить. 	<p>Студент демонстрирует:</p> <ul style="list-style-type: none"> - знание и понимание основных вопросов контролируемого объема программного материала; - твердые знания теоретического материала. - способность устанавливать и объяснять связь практики и теории, выявлять противоречия, проблемы и тенденции развития; - правильные и конкретные, без грубых ошибок, ответы на поставленные вопросы; - умение решать практические задания, которые следует выполнить. - владение основной литературой, рекомендованной программой дисциплины; - наличие собственной обоснованной позиции по обсуждаемым вопросам. <p>Возможны незначительные оговорки и неточности в раскрытии отдельных положений вопросов билета, присутствует неуверенность в ответах на дополнительные вопросы.</p>	<p>Студент демонстрирует:</p> <ul style="list-style-type: none"> - глубокие, всесторонние и аргументированные знания программного материала; - полное понимание сущности и взаимосвязи рассматриваемых процессов и явлений, точное знание основных понятий, в рамках обсуждаемых заданий; - способность устанавливать и объяснять связь практики и теории, - логически последовательные, содержательные, конкретные и исчерпывающие ответы на все задания билета, а также дополнительные вопросы экзаменатора; - умение решать практические задания. - свободное использование в ответах на вопросы материалов рекомендованной основной и дополнительной литературы.
<p>Оценка «неудовлетворительно» / «не зачтено»</p>	<p>Оценка «удовлетворительно» /зачтено</p>	<p>Оценка «хорошо»/ зачтено</p>	<p>Оценка «отлично»/ зачтено</p>

Оценка по дисциплине зависит от уровня сформированности компетенций, закрепленных за дисциплиной и представляет собой среднее арифметическое от выставленных оценок по отдельным компетенциям.

Оценка «отлично» выставляется, если среднее арифметическое находится в интервале от 4,5 до 5,0.

Оценка «хорошо» выставляется, если среднее арифметическое находится в интервале от 3,5 до 4,4.

Оценка «удовлетворительно» выставляется, если среднее арифметическое находится в интервале от 2,5 до 3,4.

Оценка «неудовлетворительно» выставляется, если среднее арифметическое находится в интервале от 0 до 2,4.

«Не зачтено» выставляется, если среднее арифметическое находится в интервале от 0 до 2,4.

«Зачтено» выставляется, если среднее арифметическое находится в интервале от 2,6 до 5,0.

8. Ресурсное обеспечение:

8.1. Перечень основной и дополнительной литературы

Основная литература:

1. Ашманов И., Касперская Н. Цифровая гигиена, Питер, 2022.
2. Бернейс Э. Манипуляция общественным мнением: как и почему // Полис. 2012. № 4
3. Богомолова Н.Н. Массовая коммуникация и общение. – М., 2009. – 300 с.
4. Богомолова Н.Н. Социальная психология печати, радио и ТВ. – М., 2010. – 632 с.
2. Браун Дж, Томпсон С. Основы воздействия СМИ. М., 2012. – 436 с.
3. Ван Дейк Т.А. Язык, познание, коммуникация. — М.: Прогресс, 2012. – 426 с.
4. Вуйма А. Чёрный PR. Защита и нападение в бизнесе и не только. — СПб: БХВ, 2005.
5. Горшков М.К. Российское общество как оно есть: опыт социологической диагностики. М.: Новый хронограф, 2011
6. Гринберг Т. Э. Политические технологии: PR и реклама. — М. : Аспект Пресс, 2006.
7. Доти Д. Паблицити и паблик рилейшнз. М., 1998. С. 86.
8. Жанры PR-текста: Учеб. пособие для студентов отделений связей с общественностью. СПб., 2012. – 540 с.
9. Зверев А.Л. ТРАНСФОРМАЦИЯ СОВРЕМЕННОГО МАССОВОГО СОЗНАНИЯ ГРАЖДАН РОССИИ Вестник Томского государственного университета Философия. Социология. Политология. 2013. № 3 (23) УДК 32.019.52
10. Зверинцев А.Б. Коммуникационный менеджмент: Рабочая книга менеджера PR. – СПб, 2012. – 336 с.
11. Зверинцев А.Б. Коммуникационный менеджмент: Рабочая книга менеджера PR. – СПб, 2013. – 240 с.
12. Комаровский В.С. Связи с общественностью в политике и государственном управлении. – РАГС, 2011. – 300 с.
13. Мансурова А.И. Манипуляция общественным сознанием посредством СМИ канд. филол. наук. Уфа, 2000
14. Меграбян А.А. О природе индивидуального сознания. Ереван, 1959 – 254 с.

15. Манойло А.В. Информационные войны и психологические операции. Руководство к действию. М., 2023.
16. Шорохова Е.В. Проблема сознания в философии и естествознании. М., 1961 – 328 с.
17. Буева Л.П. Индивидуальное сознание и условия его формирования// Вопр. филос. 1963, № 5.
18. Рубинштейн С.Л. Проблемы общей психологии. М., 1973. – 382 с.
19. Моль А. Социодинамика культуры. – М., 2013. – 337 с.
20. Образы власти в постсоветской России: политико-психологический анализ / Под ред. Е.Б. Шестопаля. М.: Алетейа, 2004.
21. Панфилова А.П. Деловая коммуникация в профессиональной деятельности. – СПб, 2012. – 553 с.
22. Первая российская PR-компания «Никколо М». Статья «Повелители выборов» апрель 2012 г.
23. Петренко В.Ф., Митина О.В. Психосемантический анализ динамики общественного сознания. Смоленск, 1997.
24. Почепцов Г. Г. Коммуникативные технологии XXI в. – М., 2013. – 330 с.
25. Почепцов Г. Г. Психологические войны. М.:«Рефл-бук», К.: «Ваклер», 2000.
26. Почепцов Г.Г. «Как пропаганда внезапно превратилась в паблик рилейшенз». 2015 г.
27. Почепцов Г.Г. Теория и практика коммуникации. – М., 2012. – 405 с.;
28. Ребане, Р Формат как средство успешной коммуникации. Опыт Эстонии
29. Сазерленд Д. SCRUM. Революционный метод управления проектами. М.,2023.
30. Секреты PR-текста: приглашение // PR-диалог. 2013. № 2 – 155 с.
31. Спиркин А. Г. Сознание и самосознание. М., Политиздат, 1972, 303 с.
32. Сэм Блэк. Паблик Рилейшнз. Что это такое? — М.: Новости, 1990
33. Федулова Ю.К. Управление общественными отношениями. М., 2011. – 647 с.
34. Филатова О.Г. Социология массовой коммуникации. М., 2013. – 453 с.
35. Хашковский А.В. Скандал! Стратегия успеха в бизнесе. - М.: Вершина, 2006
36. Цуладзе А. Большая манипулятивная игра. М.: Алгоритм, 2000. — 336 с.
37. Чалдини Р. Психология влияния. – М., 2012. – 364 с.
38. Чумиков А.Н. Связи с общественностью. М., 2010. – 300 с.
39. Эдвард Бернейс «Пропаганда» ISBN: 978-5-98999-019-1. Год издания: 2010.

8.2.Перечень лицензионного программного обеспечения (при необходимости):

Microsoft Windows 10
 Microsoft Office 2019
 Adobe Photoshop
 Adobe Audition
 Adobe After Effects
 Adobe Premier

8.3.Перечень профессиональных баз данных и информационных справочных систем:

<p>Polpred.com - Обзор СМИ https://www.polpred.com/</p>	<p>База данных с рубрикатором: 53 отрасли / 600 источников федеральных округов РФ / 235 стран и территорий / главные материалы / статьи и интервью 13000 первых лиц. Ежедневно тысяча новостей, полный текст на русском языке. Миллионы сюжетов информагентств и деловой прессы за 10 лет. Интернет-сервисы по отраслям и странам.</p>
---	--

<p>Бюро ванДайк (BvD) https://www.bvdinfo.com/ru/home?utm_campaign=search&utm_medium=cpc&utm_source=google</p>	<p>Бюро ванДайк (BvD) публикует исчерпывающую информацию о компаниях России, Украины, Казахстана всего мира, а также бизнес-аналитику.</p>
<p>Университетская информационная система РОССИЯ https://uisrussia.msu.ru/</p>	<p>Тематическая электронная библиотека и база данных прикладных исследований в области экономики, управления, социологии, лингвистики, философии, филологии, международных отношений, права.</p>
<p>Федеральная служба государственной статистики http://www.gks.ru/</p>	<p>Удовлетворение потребностей органов власти и управления, средств массовой информации, населения, научной общественности, коммерческих организаций предпринимателей, международных организаций разнообразной, объективной и полной статистической информации – главная задача Федеральной службы государственной статистики. Международная экспертиза признала статистические данные Федеральной службы государственной статистики надежными.</p>
<p>научная электронная библиотека Elibrary http://elibrary.ru/</p>	<p>Научная электронная библиотека eLIBRARY.RU - крупнейший российский информационно-аналитический портал в области науки, технологии, медицины, образования, содержащий рефераты и полные тексты более 26 млн научных статей и публикаций, в том числе электронные версии более 5600 российских научных технических журналов, из которых более 4800 журналов открытого доступа</p>
<p>портал Электронная библиотека: диссертации http://diss.rsl.ru/?menu=disscatalog/</p>	<p>Российская государственная библиотека предоставляет возможность доступа к полным текстам диссертаций, авторефератов, находящихся в электронной форме, что дает уникальную возможность многим читателям получить интересующую информацию, не покидая своего города. Доступа к ресурсам ЭБД РГБ создаются Виртуальные читальные залы в библиотеках организаций, в которых происходит просмотр электронных диссертаций, авторефератов пользователями. Каталог Электронной библиотеки диссертаций РГБ находится в свободном доступе для любого пользователя сети Интернет.</p>
<p>сайт Института научной информации по общественным наукам РАН.</p>	<p>Библиографические базы данных ИНИОН РАН по социальным и гуманитарным наукам ведутся с начала 1980-х годов. Общий объем массивов составляет более 3 млн. 500 тыс. записей (данные на 1 января 2012 г.). Ежегодно</p>

<p>http://www.inion.ru</p>	<p>прирост — около 100 тыс. записей. В базы данных включаются аннотированные описания книг и статей из журналов и сборников на 140 языков поступивших в Фундаментальную библиотеку ИНИОН РАН. Описания статей и книг в базах данных снабжены шифрами хранения и ссылками на полные тексты источников Научной электронной библиотеки.</p>
<p>Федеральный портал «Российское образование» [Электронный ресурс] – http://www.edu.ru</p>	<p>Федеральный портал «Российское образование» — уникальный интернет-ресурс в сфере образования науки. Ежедневно публикует самые актуальные новости, анонсы событий, информационные материалы для широкого круга читателей. Ежедневно на портале размещаются эксклюзивные материалы, интервью с ведущими специалистами – педагогами, психологами, учеными репортажи и аналитические статьи. Читатели получают доступ к нормативно-правовой базе сферы образования, они могут пользоваться самыми различными полезными сервисами – такими, как онлайн-тестирование, опросы по актуальным темам и т.д.</p>

8.4. Перечень ресурсов информационно-телекоммуникационной сети «Интернет» (при необходимости):

1. Центральный официальный портал Российской Федерации – сайт «Официальная Россия», размещенный по адресу <http://gov.ru>.
2. Министерство образования и науки Российской Федерации [Электронный ресурс] – Режим доступа: <http://mon.gov.ru/>;
3. Научная педагогическая библиотека им. К.Д. Ушинского [Электронный ресурс] – Режим доступа: <http://www.gnpbu.ru/>;
4. Российская государственная библиотека [Электронный ресурс] – Режим доступа: <http://www.rsl.ru/>;
5. www.evartist.ru – электронная библиотека факультета журналистики МГУ им. М.В. Ломоносова;
6. Образовательные ресурсы сети Интернет <http://book.kbsu.ru/>; <http://koob.ru/>; <http://ihtik.lib.ru/>; <http://elibrary.ru/>;
7. Федеральный портал «Российское образование» www.edu.ru/;
8. Образовательные ресурсы сети Интернет <http://book.kbsu.ru/>;
9. Библиотека Гумер (гуманитарные науки) <http://www.gumer.info/>;
10. Национальная электронная библиотека <http://нэб.рф/for-individuals/>;
11. НЭБ «Киберленинка» <http://cyberleninka.ru/>;
12. Справочно-информационный портал www.gramota.ru/;
13. Электронная библиотека Российской государственной библиотеки (РГБ) <http://elibrary.rsl.ru/>;
14. Электронная библиотека учебников <http://studentam.net/>;
15. http://www.erudition.ru/referat/printref/id.25504_1.html (Российская Электронная Библиотека «Эрудит»).

8.5. Описание материально-технического обеспечения:

Ауд. П-10

Стол преподавательский (2 шт.), стул преподавательский (2 шт.), кафедра (1 шт.), мест ученических (182 шт.), проектор BENQ (1 шт.), экран (1 шт.), ТВ Phillips (1 шт.), аудиоколонка (2шт.), доска меловая (2 шт.), компьютер (1 шт.), система оповещения (4 шт.), огнетушитель (1 шт.).

ТВ-студия 22/23

Стойка микшерная (1 шт.), шкаф телекоммуникационный (1 шт.), видеомикшер SONY (1 шт.), аудиомикшер YAMAHA (1 шт.), видеорекордер SONY (2 шт.), ноутбук Samsung (1 шт.), аудиоколонки (2 шт.), аудиомониторы (4 шт.), ТВ Samsung 55 (1 шт.), ТВ Panasonic 55 (1 шт.), стойка под ТВ (2 шт.), софиты (8 шт.), дидалайт (1 комплект), тумба металлическая (1 шт.), зеркало (1 шт.), видеосуфлер на фтативе (1 шт.), диван (1 шт.), стулья ученические (25 шт.), стулья для съемки (2 шт.), кресло преподавательское (1 шт.), стол (2 шт.), аудиоусилитель (1 шт.), стойка микрофонная (2 шт.), хаб (1 шт.), штатив для камеры (2 шт.), рабочее место ведущего (1 шт.), огнетушитель (2 шт.), система оповещения (4 шт.)

9. Язык преподавания.

Преподавание дисциплины осуществляется на русском языке.

10. Средства адаптации образовательного процесса по дисциплине к потребностям обучающихся инвалидов и лиц с ограниченными возможностями здоровья (ОВЗ)

При необходимости образовательном процессе применяются следующие методы и технологии, облегчающие восприятие информации обучающимися инвалидами и лицами с ОВЗ:

- создание текстовой версии любого нетекстового контента для его возможного преобразования в альтернативные формы, удобные для различных пользователей;
- создание контента, который можно представить в различных видах без потер данных или структуры, предусмотреть возможность масштабирования текста и изображений без потери качества;
- создание возможности для обучающихся воспринимать одну и ту же информацию из разных источников – например, так, чтобы лица с нарушением слуха получали информацию визуально, с нарушением зрения – аудиально;
- применение дистанционных образовательных технологий для передачи информации, организации различных форм интерактивной контактной работы обучающегося с преподавателем, в том числе вебинаров, которые могут быть использованы для проведения виртуальных лекций с возможностью взаимодействия всех участник дистанционного обучения, выступление с докладами и защитой выполненных работ, проведение тренингов, организации коллективной работы;
- применение дистанционных образовательных технологий для организации форм текущего и промежуточного контроля;
- увеличение продолжительности сдачи обучающимся инвалидом или лицом с ОВЗ форм промежуточной аттестации по отношению к установленной продолжительности их сдачи: зачет и экзамен, проводимый в письменной форме, - не более чем на 90 мин., проводимый в устной форме – не более чем на 20 мин.,
- продолжительности выступления обучающегося при защите курсовой работы – не более чем на 15 мин.

Факультет устанавливает конкретное содержание рабочих программ дисциплин и условия организации и проведения конкретных видов учебных занятий, составляющих

контактную работу обучающихся с преподавателем и самостоятельную работу обучающихся с ограниченными возможностями здоровья, инвалидов (при наличии факта зачисления таких обучающихся с учетом конкретных нозологий).

11. Автор (авторы) программы.

Автор рабочей программы по дисциплине «Цифровой медиапроект»: кандидат филологических наук Е.Н. Занина.