Приложение 4

к образовательной программе

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ

Б1.О.02.14 Управление цифровой репутацией и информационная безопасность

(индекс, наименование дисциплины в соответствии с учебным планом)

38.03.02 Менеджмент

(код, наименование направления подготовки/специальности)

Маркетинг

(наименование образовательной программы)

Очно-заочная форма обучения

(форма обучения)

Год набора – 2026

Донецк

Автор-составитель РПД:

Берко Анна Константиновна, канд.экон.наук, доцент, доцент кафедры маркетинга и логистики

Заведующий кафедрой:

Попова Татьяна Александровна, канд.экон.наук,доцент, заведующий кафедрой маркетинга и логистики

Рабочая программа дисциплины Б1.О.02.14 Управление цифровой репутацией и информационная безопасность одобрена на заседании кафедры маркетинга и логистики Донецкого филиала РАНХиГС.

протокол № 6 от «03» марта 2026 г.

СОДЕРЖАНИЕ

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

Дисциплина Б1.О.02.14 Управление цифровой репутацией и информационная безопасность обеспечивает формирование у обучающихся следующих универсальных и общепрофессиональных компетенций:

ОТФ/ТФ и реквизиты ПС	**Код компетенции**	**Наименование Компетенции**	**Код индикатора достижения компетенций**	**Наименование индикатора достижения компетенций**	**Образовательный результат**
ФГОС ВО бакалавриат по направлению подготовки 38.03.02 Менеджмент (Приказ Министерства науки и высшего образования Российской Федерации от 12.08.2020 г. № 970)	УК-1.	Способен осуществлять поиск, критический анализ и синтез информации, применять системный подход для решения поставленных задач	УК-2.4.	Осуществляет профессиональную деятельность в соответствии с нормами профессиональной этики и выбирает оптимальные способы решения задач, исходя из действующих правовых норм, имеющихся ресурсов и ограничений	**УК-2.4. З-4.** **Знает** нормы профессиональной этики и правовые основы работы с персональными данными и цифровой информацией в контексте управления репутацией и информационной безопасностью **УК-2.4. У-4.** **Умеет** корректировать профессиональные действия в случае изменения правовых или этических требований.
	ОПК-5.	Способен использовать при решении профессиональных задач современные информационные технологии и программные средства, включая управление крупными массивами данных и их интеллектуальный анализ.	ОПК-5.1.	Выбирает соответствующие содержанию профессиональных задач современные информационные технологии и программные средства	**ОПК-5.1. З-1.** **Знает** современные информационные технологии и программные средства для управления цифровой репутацией и обеспечения информационной безопасности. **ОПК-5.1. У-1.** **Умеет** выбирать и применять информационные технологии и программные средства для анализа профессиональных зада, оценки эффективности внедренных решений при управлении цифровой репутацией.

	ОПК-6.	Способен понимать принципы работы современных информационных технологий и использовать их для решения задач профессиональной деятельности.	ОПК-6.1.	Понимает принципы работы современных цифровых и информационных технологий, соответствующих содержанию профессиональных задач	**ОПК-6.1. З-1.** **Знает** принципы работы и области применения современных цифровых и информационных технологий в сфере управления цифровой репутацией и информационной безопасности. **ОПК-6.1. У-1.** **Умеет** применять знания о принципах работы цифровых технологий для решения профессиональных задач в области управления цифровой репутацией и информационной безопасности.

2. Объем и место дисциплины в структуре образовательной программы

Объем дисциплины

3,00 з.е., 108 ак.час

Контактная работа обучающихся с преподавателем по видам учебных занятий: 28 ак. час на контактную работу с преподавателем, из них 8 ак.час на лекции и 16 ак.час на практические занятия. 80 ак. час на самостоятельную работу обучающихся.

Б1.О.02.14 Управление цифровой репутацией и информационная безопасность реализуется на 5-м семестре 3-го курса после изучения дисциплин:

- Основы маркетингового планирования
- Методология эффективного маркетинга и управления
- Программное обеспечение маркетинговой деятельности

Форма промежуточной аттестации – зачет.

.

3. Содержание и структура дисциплины

3.1. Структура дисциплины

Очная форма обучения

№ п/п	Наименование тем и (или) разделов	Объем дисциплины, ак.час												Форма текущего контроля успеваемости, промежуточной аттестации
		ВСЕГО	Контактная работа обучающихся с преподавателем по видам учебных занятий									Самостоятельная работа		
			Период теоретического обучения						Период промежуточной аттестации (сессия)					
			Занятия лекционного типа		Занятия семинарского типа		ИК	КСР	КЭ	Каттэк	Контроль	СРкр	СРэк	СР	
			Л	ВЛ	ЛР	ПЗ									
Раздел 1. Теоретические основы управления цифровой репутацией															
Тема 1.1	Цифровая репутация как нематериальный актив компании	12	2	0	0	2	0	0	0	0		0	0	8	Опрос, тестирование
Тема 1.2	Инструменты мониторинга и анализа цифровой репутации	12	2	0	0	2	0	0	0	0		0	0	8	Опрос, задание открытого типа
Тема 1.3	Управление репутацией в социальных медиа (SERM)	8	0	0	0	0	0	0	0	0		0	0	8	Опрос, задание открытого типа
Тема 1.4	Работа с негативом и кризисные коммуникации в цифровой среде	12	2	0	0	2	0	0	0	0		0	0	8	Опрос, задание открытого типа, контрольная точка

Раздел 2. Правовые и этические основы управления цифровой репутацией и информационной безопасностью													
Тема 2.1	Правовые и этические аспекты управления цифровой репутацией	8	0	0	0	0	0	0	0	0	0	0	8	Опрос, тестирование
Тема 2.2	Основы информационной безопасности для маркетолога	8	0	0	0	0	0	0	0	0	0	0	8	Опрос, задание открытого типа
Тема 2.3	Защита персональных данных в маркетинговой деятельности	14	2	0	0	2	0	0	0	0	0	0	10	Опрос, задание открытого типа, контрольная точка
Раздел 3. Инструментарий и стратегии управления цифровой репутацией													
Тема 3.1	Программные средства для обеспечения информационной безопасности	10	0	0	0	0	0	0	0	0	0	0	10	Опрос, задание открытого типа
Тема 3.2	Интегрированная стратегия управления цифровой репутацией и информационной безопасностью	12	0	0	0	0	0	0	0	0	0	0	12	Опрос, задание открытого типа, контрольная точка
Промежуточная аттестация		4	0	0	0	0	0	0	0	4	0	0	0	Зачет
Итого		108	8	0	0	16	0	0	0	4	0	0	80	

Используемые сокращения:

Л – лекции - занятия, предусматривающие преимущественную передачу учебной информации обучающимся педагогическими работниками организации и (или) лицами, привлекаемыми организацией к реализации образовательных программ на иных условиях,).

ВЛ – видео лекции.

ЛР – лабораторные работы.

ПЗ – практические занятия (за исключением лабораторных работ).

ИК – индивидуальные консультации.

КСР – контроль самостоятельной работы

КЭ – консультации перед экзаменом

Каттэк – контактная работа на аттестацию в период экзаменационных сессий

Контроль - контактная работа на аттестацию в период экзаменационных сессий для заочной формы обучения

СРкр – самостоятельная работа на подготовку курсовой работы/ курсового проекта.

СРэк – самостоятельная работа на подготовку к экзамену.

СР – самостоятельная работа в семестре на подготовку к учебным занятиям.

3.2. Содержание дисциплины

Тема 1.1. Цифровая репутация как нематериальный актив компании (УК-2.4)

Понятие и структура цифровой репутации. Отличие цифровой репутации от бренда и имиджа. Влияние цифровой репутации на финансовые показатели компании, продажи и лояльность клиентов. Факторы, формирующие цифровую репутацию: отзывы, упоминания в СМИ и соцмедиа, рекомендации, рейтинги. Нормы профессиональной этики при работе с цифровой информацией о компании и конкурентах. Правовые основы сбора и использования информации о репутации.

Тема 1.2. Инструменты мониторинга и анализа цифровой репутации (ОПК-5.1, ОПК-6.1)

Современные информационные технологии для мониторинга упоминаний: обзор систем (Brand Analytics, IQBuzz, YouScan, СКАН-Интерфакс, Медиалогия). Принципы работы систем мониторинга социальных медиа и СМИ. Ключевые метрики оценки репутации: тональность упоминаний (позитивные, негативные, нейтральные), охват, visibility, Share of Voice, индекс репутации. Программные средства для анализа тональности текстов и выявления инфоповодов. Автоматизация сбора и обработки больших массивах данных о репутации.

Тема 1.3. Управление репутацией в социальных медиа (SERM) (УК-2.4, ОПК-5.1)

Понятие SERM (Search Engine Reputation Management) и SMM-репутация. Работа с отзывами на маркетплейсах, в картах и справочниках (2ГИС, Яндекс.Карты, Google Maps). Инструменты для управления отзывами: платформы для сбора и анализа отзывов, автоматизация ответов (CRM для репутации). Стратегии работы с негативными отзывами: стандарты ответов, эскалация, компенсация. Продвижение позитивного контента и вытеснение негатива. Нормы профессиональной этики при коммуникации с клиентами в публичной цифровой среде.

Тема 1.4. Работа с негативом и кризисные коммуникации в цифровой среде (УК-2.4)

Типология репутационных рисков и угроз в цифровой среде. Информационные атаки: хейтерские кампании, черный PR, фейковые отзывы. Раннее обнаружение репутационного кризиса. Алгоритм антикризисных коммуникаций: выявление источника негатива, оценка масштаба, выбор стратегии ответа (игнорирование, удаление, публичный ответ, юридические меры). Кейсы успешного и неудачного антикризисного управления репутацией. Корректировка профессиональных действий в случае изменения правовых или этических требований в процессе кризисных коммуникаций.

Тема 2.1. Правовые и этические аспекты управления цифровой репутацией (УК-2.4)

Правовые основы работы с информацией в сети «Интернет» в контексте управления репутацией. Федеральный закон «Об информации, информационных технологиях и о защите информации». Право на забвение: процедура удаления недостоверной информации. Ответственность за клевету и оскорбления в сети «Интернет». Этические дилеммы при управлении

репутацией: работа с фейковыми отзывами, накрутка рейтингов, скрытый маркетинг. Профессиональная этика маркетолога при сборе и использовании информации о конкурентах. Корректировка действий при изменении правовых норм.

Тема 2.2. Основы информационной безопасности для маркетолога (ОПК-5.1, ОПК-6.1)

Базовые понятия информационной безопасности: конфиденциальность, целостность, доступность информации. Основные угрозы информационной безопасности в маркетинговой деятельности: утечка баз данных клиентов, взлом аккаунтов в социальных сетях, фишинг, социальная инженерия. Принципы работы современных средств защиты информации: антивирусы, межсетевые экраны, DLP-системы, VPN. Программные средства для обеспечения безопасной работы с маркетинговыми данными. Политика безопасности при работе с корпоративной информацией в цифровой среде.

Тема 2.3. Защита персональных данных в маркетинговой деятельности (УК-2.4, ОПК-6.1)

Понятие и состав персональных данных (ПДн) в маркетинге. Федеральный закон «О персональных данных» (№ 152-ФЗ): основные требования к сбору, хранению, обработке и передаче ПДн. Принципы работы современных информационных систем для работы с ПДн. Согласие на обработку персональных данных: форма, содержание, сроки. Права субъекта персональных данных. Ответственность за утечку и неправомерную обработку ПДн. Нормы профессиональной этики при сборе и использовании данных клиентов. Корректировка маркетинговых действий при изменении требований законодательства о ПДн.

Тема 3.1. Программные средства для обеспечения информационной безопасности (ОПК-5.1, ОПК-6.1)

Обзор программных средств для защиты маркетинговой деятельности: антивирусные решения, средства шифрования данных, менеджеры паролей, VPN-сервисы, DLP-системы. Принципы работы средств многофакторной аутентификации. Инструменты для безопасного хранения и передачи маркетинговых данных (облачные хранилища с шифрованием). Выбор оптимальных программных средств для решения конкретных задач управления цифровой репутацией и обеспечения информационной безопасности. Оценка эффективности внедренных решений.

Тема 3.2. Интегрированная стратегия управления цифровой репутацией и информационной безопасностью (УК-2.4, ОПК-5.1, ОПК-6.1)

Разработка стратегии управления цифровой репутацией компании: цели, KPI, целевые показатели. Интеграция управления репутацией с информационной безопасностью и маркетинговой стратегией. Регламенты работы с репутационными рисками и информационными угрозами. Обучение сотрудников правилам цифровой гигиены и репутационной безопасности. Использование современных информационных технологий и программных средств для мониторинга, анализа и защиты репутации. Оценка эффективности внедренных решений и корректировка стратегии в соответствии с изменяющимися правовыми и этическими требованиями.

4. Типы оценочных материалов, показатели и критерии оценивания

4.1. Оценочные материалы по дисциплине Б1.О.02.14 Управление цифровой репутацией и информационная безопасность входят в состав оценочных материалов по образовательной программе. Совокупность оценочных материалов по всем дисциплинам (модулям) образовательной программы составляет фонд оценочных средств (далее – ФОС). ФОС используется при проведении текущего контроля успеваемости и промежуточной аттестации обучающихся с целью оценивания достижения обучающимися планируемых результатов обучения.

4.2. ФОС разработан как комплекс проверочных заданий различного типа и уровня сложности, включает критерии и шкалы оценивания, а также «ключи» правильных ответов. ФОС формируется как отдельный документ и хранится в электронном виде, доступ к ФОС предоставлен ограниченному кругу лиц.

4.3. Для самостоятельной работы обучающихся при подготовке к текущему контролю успеваемости и промежуточной аттестации в рабочих программах дисциплин размещены типовые проверочные задания, которые можно условно разделить на задания закрытого, комбинированного и открытого типов.

Задания закрытого типа — это тестовые задания, в которых каждый вопрос сопровождается готовыми вариантами ответов, из которых необходимо выбрать один или несколько правильных.

Задания комбинированного типа – это тестовые задания, в которых каждый вопрос сопровождается готовыми вариантами ответов, из которых необходимо выбрать один или несколько правильных и обосновать свой выбор.

Задания открытого типа — это задания, в которых на каждый вопрос должен быть предложен развернутый обоснованный ответ.

В зависимости от типа задания рекомендованы определенная последовательность выполнения и система оценивания выполнения заданий.

4.4. Типы заданий, сценарии выполнения, критерии оценивания

ТИП ЗАДАНИЯ	ИНСТРУКЦИЯ	СЦЕНАРИИ ВЫПОЛНЕНИЯ	КРИТЕРИИ ОЦЕНИВАНИЯ
Задание закрытого типа с выбором одного правильного ответа из нескольких вариантов предложенных	Прочитайте текст, выберите правильный ответ	1. Внимательно прочитать текст задания и понять, что в качестве ответа ожидается только один из предложенных вариантов. 2. Внимательно прочитать предложенные вариант-ты ответа. 3. Выбрать один верный ответ. 4. Записать только номер (или букву) выбранного варианта ответа (например, 3 или В).	Ответ считается верным, если правильно указана цифра или буква
Задание закрытого типа на установление соответствия	Прочитайте текст и установите соответствие	1. Внимательно прочитать текст задания и понять, что в качестве ответа ожидаются пары элементов. 2. Внимательно прочитать оба списка: список 1 – вопросы, утверждения, факты, понятия и т.д.; список 2 – утверждения, свойства объектов и т.д. 3. Сопоставить элементы списка 1 с элементами списка 2, сформировать пары элементов. 4. Записать попарно буквы и цифры (в зависимости от задания) вариантов ответа (например, А1 или Б4).	Ответ считается верным, если правильно указаны цифры или буквы
Задание закрытого типа с выбором нескольких правильных ответов из нескольких вариантов предложенных	Прочитайте текст, выберите правильные ответы	1. Внимательно прочитать текст задания и понять, что в качестве ответа ожидается несколько правильных ответов из предложенных вариантов. 2. Внимательно прочитать предложенные вариант-ты ответа. 3. Выбрать несколько правильных ответов. 4. Записать только номера (или буквы) выбранного варианта ответа (например, 1 4 или А Г).	Ответ считается верным, если правильно установлены все соответствия (позиции из одного столбца верно сопоставлены с позициями другого)

Задание закрытого типа на установление последовательности	Прочитайте текст и установите последовательность	1. Внимательно прочитать текст задания и понять, что в качестве ответа ожидается последовательность элементов. 2. Внимательно прочитать предложенные варианты ответа. 3. Построить верную последовательность из предложенных элементов. 4. Записать буквы/цифры (в зависимости от задания) вариантов ответа в нужной последовательности (например, БВА или 135).	Ответ считается верным, если правильно указана вся последовательность цифр
Задание комбинированного типа с выбором одного правильного ответа из предложенных и обоснованием выбора	Прочитайте текст, выберите правильный ответ и запишите аргументы, обосновывающие выбор ответа	1. Внимательно прочитать текст задания и понять, что в качестве ответа ожидается только один из предложенных вариантов. 2. Внимательно прочитать предложенные варианты ответа. 3. Выбрать один верный ответ. 4. Записать только номер (или букву) выбранного варианта ответа. 5. Записать аргументы, обосновывающие выбор ответа (например, 4 текст обоснования).	Ответ считается верным, если правильно указана цифра или буква и приведены корректные аргументы, используемые при выборе ответа
Задание открытого типа с развернутым ответом	Прочитайте текст и запишите развернутый обоснованный ответ	1. Внимательно прочитать текст задания и понять суть вопроса. 2. Продумать логику и полноту ответа. 3. Записать ответ, используя четкие компактные формулировки. 4. В случае расчетной задачи, записать решение и ответ	Ответ считается верным: 1. Отсутствие фактических ошибок. 2. Раскрытие объема используемых понятий (полнота ответа). 3. Обоснованность ответа (наличие аргументов). 4. Логическая последовательность излагаемого материала.

4.5. Общая шкала оценивания результатов текущего контроля успеваемости и промежуточной аттестации обучающихся с применением БРС

Итоговая балльная оценка	**Традиционная система**	**Бинарная система**	**ECTS**	
			Для традиционной системы	**Для бинарной системы**
90-100	Отлично	Зачтено	A	P/ Passed
80-89	Хорошо		B	P/ Passed
75-79			C	P/ Passed
70-74	Удовлетворительно		D	P/ Passed
60-69			E	P/ Passed
0-59	Неудовлетворительно	Не зачтено	F	F/Failed

Соотношение баллов за текущий контроль успеваемости и промежуточную аттестацию, а также повторную промежуточную аттестацию:

Максимальная сумма баллов за текущий контроль успеваемости	Максимальная сумма баллов за промежуточную аттестацию	Максимальная итоговая балльная оценка	Максимальная сумма баллов за повторную промежуточную аттестацию
100 баллов	100 баллов	100 баллов	100 баллов

5. Формы аттестации, типовые оценочные материалы для текущего контроля успеваемости обучающихся, критерии и шкалы оценивания по контрольным точкам

5.1. В ходе реализации дисциплины Б1.О.02.14 Управление цифровой репутацией и информационная безопасность используются следующие формы текущего контроля успеваемости обучающихся (в том числе, задания к контрольным точкам):

опрос, тестирование, задание открытого типа

5.2. Типовые оценочные материалы для текущего контроля успеваемости обучающихся (вне контрольных точек):

Тема 1.1. Цифровая репутация как нематериальный актив компании (УК-2.4)

Вопросы для опроса:

1. Что такое цифровая репутация? Чем она отличается от бренда и имиджа?
2. Какие факторы влияют на формирование цифровой репутации компании?
3. Как цифровая репутация влияет на финансовые показатели компании, продажи и лояльность клиентов?
4. Какие нормы профессиональной этики необходимо соблюдать при работе с цифровой информацией о компании и конкурентах?
5. Какие правовые ограничения существуют при сборе и использовании

информации о репутации третьих лиц?

Тестовые задания:

Внимательно прочитайте текст задания и выберите один правильный ответ из предложенных вариантов. Запишите букву выбранного варианта ответа.

1. Что из перечисленного НЕ является фактором, формирующим цифровую репутацию?

А) отзывы клиентов

Б) упоминания в СМИ

В) цветовая гамма логотипа

Г) рейтинги на маркетплейсах

2. Какой показатель отражает долю упоминаний компании в общем объеме упоминаний всех игроков рынка?

А) охват

Б) тональность

В) Share of Voice

Г) индекс репутации

3. Что из перечисленного относится к нематериальным активам компании?

А) основные средства

Б) цифровая репутация

В) оборотные средства

Г) запасы готовой продукции

Задание открытого типа:

Прочитайте текст задания и запишите развернутый обоснованный ответ.

1. Проанализируйте цифровую репутацию любой известной компании по вашему выбору. Какие факторы оказывают наибольшее влияние на ее репутацию? Какие репутационные риски вы видите? Предложите рекомендации по улучшению репутации.

2. Составьте чек-лист «Правила профессиональной этики маркетолога при работе с цифровой информацией» (не менее 10 пунктов).

Тема 1.2. Инструменты мониторинга и анализа цифровой репутации (ОПК-5.1, ОПК-6.1)

Вопросы для опроса:

1. Какие системы мониторинга цифровой репутации существуют на российском рынке?

2. Каковы принципы работы систем мониторинга социальных медиа и СМИ?

3. Какие метрики используются для оценки цифровой репутации?

4. Что такое тональность упоминаний и как она определяется?

5. Как происходит автоматизация сбора и обработки больших массивов данных о репутации?

Тестовые задания:

Внимательно прочитайте текст задания и выберите один правильный ответ из предложенных вариантов. Запишите букву выбранного варианта ответа.

1. Какой сервис предназначен для мониторинга и анализа цифровой репутации?

А) PowerPoint
Б) Brand Analytics
В) Excel
Г) 1С:Бухгалтерия

2. Что показывает метрика «охват» (reach)?
А) количество упоминаний компании
Б) количество уникальных пользователей, увидевших упоминание
В) долю упоминаний компании на рынке
Г) соотношение позитивных и негативных отзывов

3. Что такое «индекс репутации»?
А) количество подписчиков в социальных сетях
Б) интегральный показатель, учитывающий различные параметры репутации
В) количество упоминаний в СМИ за месяц
Г) цена акций компании

Задание открытого типа:

Прочитайте текст задания и запишите развернутый обоснованный ответ.

1. Проведите анализ цифровой репутации компании (по выбору) с использованием открытых данных. Оцените тональность упоминаний, охват, ключевые инфоповоды за последний месяц. Результаты оформите в виде отчета.

2. Заполните таблицу «Сравнительный анализ систем мониторинга цифровой репутации (Brand Analytics, IQBuzz, YouScan, Медиалогия)» по критериям: функциональность, стоимость, удобство, охват источников.

Тема 1.3. Управление репутацией в социальных медиа (SERM) (УК-2.4, ОПК-5.1)

Вопросы для опроса:

1. Что такое SERM (Search Engine Reputation Management) и SMM-репутация?
2. Какие каналы и площадки наиболее важны для управления цифровой репутацией?
3. Как работать с отзывами на маркетплейсах (Wildberries, Ozon, Яндекс.Маркет)?
4. Какие существуют стратегии работы с негативными отзывами?
5. Какие инструменты позволяют автоматизировать управление отзывами?

Тестовые задания:

Внимательно прочитайте текст задания и выберите один правильный ответ из предложенных вариантов. Запишите букву выбранного варианта ответа.

1. Что означает аббревиатура SERM?
А) управление репутацией в поисковых системах
Б) управление продажами в социальных сетях
В) управление персоналом компании
Г) управление бюджетом маркетинга

2. Какая стратегия работы с негативным отзывом предполагает отсутствие публичной реакции, если отзыв необоснованный?
А) удаление
Б) эскалация
В) игнорирование

Г) публичный ответ

3. Что из перечисленного относится к инструментам управления отзывами?

А) CRM для репутации

Б) ERP-система

В) текстовый редактор

Г) графический редактор

Задание открытого типа:

Прочитайте текст задания, проанализируйте предложенную ситуацию. Дайте развернутый обоснованный ответ.

1. Компания получила на маркетплейсе негативный отзыв: «Товар пришел с браком, служба поддержки не отвечает на сообщения уже третий день. Деньги потрачены зря. Не рекомендую!» Разработайте алгоритм действий: как ответить на отзыв? Какие меры предпринять дополнительно? Напишите текст ответа.

2. Вы обнаружили на форуме обсуждение вашей компании, в котором пользователи активно делятся негативным опытом, хотя реальных претензий не поступало. Какова ваша стратегия? Предложите пошаговый план действий.

Тема 1.4. Работа с негативом и кризисные коммуникации в цифровой среде (УК-2.4)

Вопросы для опроса:

1. Какие виды репутационных рисков и угроз существуют в цифровой среде?

2. Что такое информационная атака? Приведите примеры.

3. Каков алгоритм антикризисных коммуникаций?

4. Какие стратегии ответа на негатив могут быть использованы в кризисной ситуации?

5. Как корректировать профессиональные действия при изменении правовых или этических требований в процессе кризисных коммуникаций?

Тестовые задания:

Внимательно прочитайте текст задания и выберите один правильный ответ из предложенных вариантов. Запишите букву выбранного варианта ответа.

1. Что из перечисленного является информационной атакой?

А) позитивный отзыв клиента

Б) хейтерская кампания

В) новость о запуске продукта

Г) исследование рынка

2. Какой метод работы с негативом предполагает отсутствие публичной реакции?

А) удаление

Б) публичный ответ

В) игнорирование

Г) юридические меры

3. Что является первым этапом антикризисных коммуникаций?

А) выбор стратегии ответа

Б) публичное заявление

В) мониторинг и раннее обнаружение кризиса

Г) оценка ущерба

Задание открытого типа:

Прочитайте текст задания, проанализируйте предложенную ситуацию. Дайте развернутый обоснованный ответ.

1. В социальных сетях и СМИ стремительно распространяется информация о том, что ваша компания использует некачественное сырье. Информация не подтверждена, но уже нанесен урон репутации. Разработайте антикризисный план действий: какие шаги предпринять в первые 24 часа, 48 часов, неделю?

2. Проанализируйте кейс успешного антикризисного управления репутацией любой известной компании. Выделите ключевые факторы успеха. Опишите, какие ошибки были допущены в кейсе неудачного антикризисного управления (по выбору).

Тема 2.1. Правовые и этические аспекты управления цифровой репутацией (УК-2.4)

Вопросы для опроса:

1. Какие правовые нормы регулируют работу с информацией в сети «Интернет» в контексте управления репутацией?

2. Что такое «право на забвение» и какова процедура удаления недостоверной информации?

3. Какая ответственность предусмотрена за клевету и оскорбления в сети «Интернет»?

4. Какие этические дилеммы возникают при управлении цифровой репутацией?

5. Как корректировать профессиональные действия при изменении правовых норм в сфере информационной безопасности?

Тестовые задания:

Внимательно прочитайте текст задания и выберите один правильный ответ из предложенных вариантов. Запишите букву выбранного варианта ответа.

1. Какой Федеральный закон является основным в сфере регулирования информации в сети «Интернет»?

А) Федеральный закон «О рекламе»

Б) Федеральный закон «Об информации, информационных технологиях и о защите информации»

В) Федеральный закон «О защите прав потребителей»

Г) Федеральный закон «О конкуренции»

2. Что такое «право на забвение»?

А) право компании удалить любой негативный отзыв

Б) право гражданина требовать удаления недостоверной информации о себе из поисковых систем

В) право маркетолога игнорировать запросы клиентов

Г) право СМИ не раскрывать источники информации

3. Какая статья КоАП РФ предусматривает ответственность за оскорбление в сети «Интернет»?

А) 1.1

Б) 5.61

В) 10.5

Г) 13.15

Тестовые задания:

Прочитайте текст задания, выберите несколько правильных ответов из предложенных вариантов. Запишите буквы выбранных вариантов ответа.

4. Какие действия являются нарушением профессиональной этики маркетолога при управлении цифровой репутацией? (Выберите несколько)

А) написание фейковых положительных отзывов о своей компании

Б) накрутка рейтингов с помощью ботов

В) сбор и анализ открытых отзывов клиентов

Г) черный PR в отношении конкурентов

Д) публикация достоверной информации о своей компании

Тема 2.2. Основы информационной безопасности для маркетолога (ОПК-5.1, ОПК-6.1)

Вопросы для опроса:

1. Каковы основные угрозы информационной безопасности в маркетинговой деятельности?

2. Что такое фишинг и социальная инженерия? Приведите примеры.

3. Какие существуют виды средств защиты информации (антивирусы, межсетевые экраны, DLP-системы, VPN)?

4. Что такое политика безопасности при работе с корпоративной информацией в цифровой среде?

5. Каковы принципы работы средств многофакторной аутентификации?

Тестовые задания:

Внимательно прочитайте текст задания и выберите один правильный ответ из предложенных вариантов. Запишите букву выбранного варианта ответа.

1. Что из перечисленного относится к базовым понятиям информационной безопасности?

А) конфиденциальность, целостность, доступность

Б) скорость, точность, надежность

В) качество, количество, стоимость

Г) дизайн, эргономика, стиль

2. Что такое фишинг?

А) вид компьютерного вируса

Б) вид мошенничества с целью получения конфиденциальных данных

В) метод защиты информации

Г) антивирусная программа

3. Для чего используются DLP-системы?

А) для создания презентаций

Б) для предотвращения утечек конфиденциальных данных

В) для мониторинга социальных сетей

Г) для управления репутацией

Задание открытого типа:

Прочитайте текст задания и запишите развернутый обоснованный ответ.

1. Разработайте памятку для сотрудников отдела маркетинга «Правила цифровой гигиены и информационной безопасности» (не менее 15 пунктов). Включите рекомендации по работе с паролями, фишинговыми письмами, публичным

Wi-Fi, социальными сетями.

2. Проанализируйте типовое фишинговое письмо (образец предоставляется преподавателем). Выявите признаки, указывающие на мошеннический характер письма. Предложите алгоритм действий для сотрудника, получившего такое письмо.

Тема 2.3. Защита персональных данных в маркетинговой деятельности (УК-2.4, ОПК-6.1)

Вопросы для опроса:

1. Что такое персональные данные согласно Федеральному закону № 152-ФЗ?
2. Какие требования предъявляются к сбору, хранению, обработке и передаче персональных данных?
3. Что должно содержать согласие на обработку персональных данных?
4. Какие права имеют субъекты персональных данных?
5. Какая ответственность предусмотрена за утечку и неправомерную обработку персональных данных?

Тестовые задания:

Внимательно прочитайте текст задания и выберите один правильный ответ из предложенных вариантов. Запишите букву выбранного варианта ответа.

1. Какой Федеральный закон регулирует вопросы обработки персональных данных?

А) № 38-ФЗ «О рекламе»
Б) № 152-ФЗ «О персональных данных»
В) № 149-ФЗ «Об информации...»
Г) № 135-ФЗ «О защите конкуренции»

2. Что из перечисленного НЕ относится к персональным данным?

А) фамилия, имя, отчество
Б) дата и место рождения
В) ИНН компании
Г) адрес места жительства

3. Что должно содержать согласие на обработку персональных данных?

А) только подпись субъекта
Б) цель обработки, перечень данных, срок действия, подпись
В) только перечень данных

Задание открытого типа:

Прочитайте текст задания и запишите развернутый обоснованный ответ.

1. Проанализируйте форму сбора персональных данных на сайте любой компании (форма подписки на рассылку, форма регистрации, форма обратной связи). Оцените ее соответствие требованиям Федерального закона № 152-ФЗ. Выявите недостатки и предложите рекомендации по улучшению.

2. Составьте шаблон согласия на обработку персональных данных для интернет-магазина. Включите все обязательные элементы, предусмотренные законодательством.

3. Компания планирует передать базу данных клиентов стороннему подрядчику для проведения маркетингового исследования. Какие юридические действия необходимо совершить компании? Какие документы должны быть оформлены? Ответьте развернуто со ссылками на законодательство.

Тема 3.1. Программные средства для обеспечения информационной безопасности (ОПК-5.1, ОПК-6.1)

Вопросы для опроса:

1. Какие классы программных средств для обеспечения информационной безопасности вы знаете?
2. Какие задачи решают антивирусные решения? Назовите примеры.
3. Для чего используются средства шифрования данных? Приведите примеры.
4. Что такое многофакторная аутентификация и как она работает?
5. Какие критерии следует учитывать при выборе программных средств для информационной безопасности?

Тестовые задания:

Внимательно прочитайте текст задания и выберите один правильный ответ из предложенных вариантов. Запишите букву выбранного варианта ответа.

1. Для чего предназначены антивирусные программы?
   А) для создания презентаций
   Б) для обнаружения и удаления вредоносного программного обеспечения
   В) для мониторинга социальных сетей
   Г) для управления репутацией
2. Что такое VPN?
   А) антивирусная программа
   Б) технология, создающая зашифрованное соединение между устройством и сетью
   В) программное обеспечение для управления проектами
   Г) система мониторинга социальных сетей
3. Что относится к средствам многофакторной аутентификации?
   А) пароль
   Б) пароль + код из SMS
   В) только биометрические данные
   Г) только push-уведомление

Задание открытого типа:

Прочитайте текст задания и запишите развернутый обоснованный ответ.

1. Заполните таблицу «Сравнительный анализ антивирусных решений (Kaspersky, Dr.Web, ESET NOD32)» по критериям: функциональность, стоимость, удобство, влияние на производительность системы.
2. Подготовьте обоснование выбора программных средств для информационной безопасности для малого интернет-магазина. Укажите, какие средства защиты необходимы и почему.

Задания на установление соответствия:

Прочитайте текст задания. Сопоставьте элементы списка 1 с элементами списка 2, сформируйте пары элементов. Запишите попарно буквы и цифры (например, А1, Б2).

Установите соответствие между программным средством и его назначением:

Список 1 (Программное средство)	Список 2 (Назначение)
А) Менеджер паролей	1) Безопасное подключение к сети через зашифрованное соединение
Б) DLP-система	2) Управление учетными данными и создание сложных паролей
В) VPN-сервис	3) Предотвращение утечек конфиденциальных данных
Г) Антивирус	4) Обнаружение и удаление вредоносного ПО

Тема 3.2. Интегрированная стратегия управления цифровой репутацией и информационной безопасностью (УК-2.4, ОПК-5.1, ОПК-6.1)

Вопросы для опроса:

1. Как разработать стратегию управления цифровой репутацией компании? Какие элементы она включает?
2. Какие KPI и целевые показатели используются для оценки эффективности управления репутацией?
3. Как интегрировать управление репутацией с информационной безопасностью и маркетинговой стратегией?
4. Какие регламенты необходимо разработать для работы с репутационными рисками?
5. Как обучить сотрудников правилам цифровой гигиены и репутационной безопасности?

Тестовые задания:

Внимательно прочитайте текст задания и выберите один правильный ответ из предложенных вариантов. Запишите букву выбранного варианта ответа.

1. Какой показатель НЕ относится к KPI управления цифровой репутацией?

А) рост доли позитивных упоминаний

Б) увеличение количества подписчиков в социальных сетях

В) количество внутренних приказов

Г) снижение времени реакции на негатив

2. Что из перечисленного должно входить в регламент работы с репутационными рисками?

А) порядок действий при выявлении негатива

Б) рецепты блюд в столовой

В) расписание отпусков сотрудников

Г) технические характеристики продукции

3. Как часто рекомендуется пересматривать стратегию управления цифровой репутацией?

А) один раз в 10 лет

Б) регулярно, с учетом изменения правовых и этических требований

В) только при смене руководителя

Г) никогда

Задание открытого типа:

Прочитайте текст задания, проанализируйте предложенную ситуацию. Дайте развернутый обоснованный ответ.

1. Разработайте интегрированную стратегию управления цифровой репутацией

для сети кофеен (или другой компании по выбору). Определите цели, KPI, ключевые мероприятия, бюджет (укрупненно), ответственных, сроки. Оформите в виде плана-стратегии.

2. Составьте план обучения сотрудников отдела маркетинга правилам цифровой гигиены и репутационной безопасности. Включите темы, форматы, периодичность обучения, способы контроля усвоения материала.

3. Опишите, как может быть интегрирована система мониторинга цифровой репутации с системой информационной безопасности компании. Какие данные могут быть общими? Как взаимодействуют ответственны должностные лица?

4. Разработайте памятку для сотрудников колл-центра «Как правильно общаться с клиентами в социальных сетях и не навредить репутации компании» (не менее 10 правил).

Критерии оценивания опроса:

Баллы	Описание критерия
3	Обучающийся полно излагает материал (отвечает на вопрос), дает правильное определение основных понятий; обнаруживает понимание материала, может обосновать свои суждения, применить знания на практике, привести необходимые примеры не только из учебника, но и самостоятельно составленные; излагает материал последовательно и правильно с точки зрения норм литературного языка.
2	Обучающийся дает ответ, удовлетворяющий тем же требованиям, что и для оценки «отлично», но допускает 1–2 ошибки, которые сам же исправляет, и 1–2 недочета в последовательности и языковом оформлении излагаемого.
1	Обучающийся обнаруживает знание и понимание основных положений данной темы, но излагает материал неполно и допускает неточности в определении понятий или формулировке правил; не умеет достаточно глубоко и доказательно обосновать свои суждения и привести свои примеры; излагает материал непоследовательно и допускает ошибки в языковом оформлении излагаемого.
0	Обучающийся обнаруживает незнание вопроса, допускает ошибки в формулировке определений и правил, искажающие их смысл, беспорядочно и неуверенно излагает материал.

0* - в журнал академической группы не выставляется

Критерии оценивания тестовых заданий:

Баллы	Описание критерия	
2	Свыше 80% правильных ответов.	Обучающийся демонстрирует глубокое познание в освоенном материале.
1	Свыше 50% правильных ответов.	Обучающимся материал освоен не полностью, имеются значительные пробелы в знаниях.
0	Менее 50% правильных ответов.	Обучающимся материал не освоен, знания обучающегося ниже базового уровня.

0* - в журнал академической группы не выставляется

Критерии оценивания заданий открытого типа с развернутым ответом:

Баллы	Описание критерия
3	Обучающийся полно излагает материал (отвечает на вопрос), дает правильное определение основных понятий; обнаруживает понимание материала, может обосновать свои суждения, применить знания на практике, привести необходимые примеры не только из учебника, но и самостоятельно составленные; излагает материал последовательно и правильно с точки зрения норм литературного языка.
2	Обучающийся дает ответ, удовлетворяющий тем же требованиям, что и для оценки «отлично», но допускает 1–2 ошибки, которые сам же исправляет, и 1–2 недочета в последовательности и языковом оформлении излагаемого.
1	Обучающийся обнаруживает знание и понимание основных положений данной темы, но излагает материал неполно и допускает неточности в определении понятий или формулировке правил; не умеет достаточно глубоко и доказательно обосновать свои суждения и привести свои примеры; излагает материал непоследовательно и допускает ошибки в языковом оформлении излагаемого.
0	Обучающийся обнаруживает незнание вопроса, допускает ошибки в формулировке определений и правил, искажающие их смысл, беспорядочно и неуверенно излагает материал.

0* - в журнал академической группы не выставляется

5.3. Один или несколько тематических блоков дисциплины завершаются контрольной точкой (далее – КТ). Текущий контроль успеваемости по дисциплине предусматривает не менее 2 (двух) и не более 10 (десяти) КТ в течение периода освоения дисциплины.

Наименование контрольной точки	Максимальное количество баллов за работу в рамках КТ, которое может набрать студент
КТ 1	10
КТ 2	10
КТ 3	10
Итого:	30

5.4. Формы текущего контроля успеваемости обучающихся в рамках КТ и типовые оценочные материалы:

КТ — 1. Раздел 1 (темы 1.1, 1.2, 1.3, 1.4)

Задание закрытого типа с выбором одного правильного ответа

Прочитайте текст задания, выберите один правильный ответ из предложенных вариантов. Запишите букву выбранного варианта ответа.

1. Что из перечисленного относится к инструментам мониторинга цифровой репутации?

А) CRM-система

Б) Brand Analytics

В) ERP-система

Г) текстовый редактор

2. Какой показатель отражает долю упоминаний компании в общем объеме упоминаний всех игроков рынка?

А) охват
Б) тональность
В) Share of Voice
Г) индекс репутации

3. Что означает аббревиатура SERM?
А) управление репутацией в поисковых системах
Б) управление продажами в социальных сетях
В) управление персоналом компании
Г) управление бюджетом маркетинга

4. Какая стратегия работы с негативным отзывом предполагает отсутствие публичной реакции, если отзыв необоснованный?
А) удаление
Б) эскалация
В) игнорирование
Г) публичный ответ

5. Что из перечисленного является информационной атакой?
А) позитивный отзыв клиента
Б) хейтерская кампания
В) новость о запуске продукта
Г) исследование рынка

Задание закрытого типа на установление соответствия

Прочитайте текст задания. Сопоставьте элементы списка 1 с элементами списка 2, сформируйте пары элементов. Запишите попарно буквы и цифры (например, А1, Б2).

6. Установите соответствие между метрикой оценки репутации и ее описанием:

Список 1 (Метрика)	Список 2 (Описание)
А) Охват	1) Доля упоминаний компании в общем объеме упоминаний всех игроков рынка
Б) Тональность	2) Количество уникальных пользователей, увидевших упоминание
В) Share of Voice	3) Соотношение позитивных, негативных и нейтральных отзывов
Г) Индекс репутации	4) Интегральный показатель, учитывающий различные параметры репутации

7. Установите соответствие между типом репутационного риска и его описанием:

Список 1 (Тип риска)	Список 2 (Описание)
А) Информационная атака	1) Публикация фейковых негативных отзывов конкурентами
Б) Хейтерская кампания	2) Систематические нападки на бренд в социальных сетях
В) Черный PR	3) Целенаправленное распространение ложной информации для подрыва репутации
Г) Репутационный кризис	4) Резкое ухудшение репутации под влиянием негативных событий

Задание закрытого типа с выбором нескольких правильных ответов

Прочитайте текст задания, выберите несколько правильных ответов из предложенных вариантов. Запишите буквы выбранных вариантов ответа (например, А, Б, В).

8. Какие факторы формируют цифровую репутацию компании? (Выберите

несколько)

А) отзывы клиентов на маркетплейсах

Б) упоминания в социальных медиа

В) внутренняя документация компании

Г) рейтинги в картах и справочниках

Д) расписание работы офиса

9. Какие стратегии ответа на негатив могут быть использованы в кризисных коммуникациях? (Выберите несколько)

А) игнорирование

Б) удаление

В) публичный ответ

Г) юридические меры

Д) накрутка позитивных отзывов

Задание закрытого типа на установление последовательности

Прочитайте текст задания. Постройте верную последовательность из предложенных элементов. Запишите буквы в нужном порядке (например, А, Б, В, Г).

10. Установите правильную последовательность этапов антикризисных коммуникаций в цифровой среде:

А) Оценка масштаба кризиса

Б) Выбор стратегии ответа

В) Мониторинг и раннее обнаружение кризиса

Г) Выявление источника негатива

Д) Реализация выбранной стратегии

11. Установите правильную последовательность действий при работе с негативным отзывом на маркетплейсе:

А) Публичный ответ на отзыв

Б) Анализ причины недовольства

В) Принесение извинений

Г) Предложение решения проблемы

Д) Благодарность за обратную связь

Задание открытого типа с развернутым ответом (ситуационное задание)

Прочитайте текст задания, проанализируйте предложенную ситуацию. Дайте развернутый обоснованный ответ.

12. Компания «ВкусДома» — крупный производитель замороженных полуфабрикатов. В социальных сетях массово распространяются видео, на которых неизвестные люди находят в продуктах компании посторонние предметы. Внутреннее расследование установило, что видеоролики являются смонтированными.

Вопросы:

1. Какой тип репутационного кризиса возник у компании? (Оцените по масштабу и времени развития).

2. Разработайте пошаговый план действий компании в первые 24 часа (распишите по временным интервалам).

3. Напишите текст публичного заявления компании в социальных сетях.

КТ — 2. Раздел 2 (темы 2.1, 2.2, 2.3)

Задание закрытого типа с выбором одного правильного ответа

Прочитайте текст задания, выберите один правильный ответ из предложенных вариантов. Запишите букву выбранного варианта ответа.

1. Какой Федеральный закон является основным в сфере регулирования информации в сети «Интернет»?

А) Федеральный закон «О рекламе»

Б) Федеральный закон «Об информации, информационных технологиях и о защите информации»

В) Федеральный закон «О защите прав потребителей»

Г) Федеральный закон «О конкуренции»

2. Что такое фишинг?

А) вид компьютерного вируса

Б) вид мошенничества с целью получения конфиденциальных данных

В) метод защиты информации

Г) антивирусная программа

3. Какой Федеральный закон регулирует вопросы обработки персональных данных?

А) № 38-ФЗ «О рекламе»

Б) № 152-ФЗ «О персональных данных»

В) № 149-ФЗ «Об информации...»

Г) № 135-ФЗ «О защите конкуренции»

4. Что из перечисленного относится к базовым понятиям информационной безопасности?

А) конфиденциальность, целостность, доступность

Б) скорость, точность, надежность

В) качество, количество, стоимость

Г) дизайн, эргономика, стиль

5. Что такое «право на забвение»?

А) право компании удалить любой негативный отзыв

Б) право гражданина требовать удаления недостоверной информации о себе из поисковых систем

В) право маркетолога игнорировать запросы клиентов

Г) право СМИ не раскрывать источники информации

Задание закрытого типа на установление соответствия

Прочитайте текст задания. Сопоставьте элементы списка 1 с элементами списка 2, сформируйте пары элементов. Запишите попарно буквы и цифры (например, А1, Б2).

6. Установите соответствие между программным средством и его назначением:

Список 1 (Программное средство)	Список 2 (Назначение)
А) Менеджер паролей	1) Безопасное подключение к сети через зашифрованное соединение
Б) DLP-система	2) Управление учетными данными и создание сложных паролей
В) VPN-сервис	3) Предотвращение утечек конфиденциальных данных

Г) Антивирус	4) Обнаружение и удаление вредоносного ПО

7. Установите соответствие между видом ответственности и ее характеристикой:

Список 1 (Вид ответственности)	Список 2 (Характеристика)
А) Административная	1) Штрафы по КоАП РФ, приостановление деятельности
Б) Гражданско-правовая	2) Возмещение убытков, компенсация морального вреда
В) Уголовная	3) Лишение свободы, крупные штрафы по УК РФ
Г) Дисциплинарная	4) Выговор, увольнение по инициативе работодателя

Задание закрытого типа с выбором нескольких правильных ответов

Прочитайте текст задания, выберите несколько правильных ответов из предложенных вариантов. Запишите буквы выбранных вариантов ответа (например, А, Б, В).

8. Какие действия являются нарушением профессиональной этики маркетолога при управлении цифровой репутацией? (Выберите несколько)

А) написание фейковых положительных отзывов о своей компаний

Б) накрутка рейтингов с помощью ботов

В) сбор и анализ открытых отзывов клиентов

Г) черный PR в отношении конкурентов

Д) публикация достоверной информации о своей компании

9. Какие меры относятся к организационным мерам защиты персональных данных? (Выберите несколько)

А) назначение ответственного за обработку ПДн

Б) установка антивируса

В) разработка политики обработки ПДн

Г) шифрование баз данных

Д) обучение сотрудников правилам работы с ПДн

Задание закрытого типа на установление последовательности

Прочитайте текст задания. Постройте верную последовательность из предложенных элементов. Запишите буквы в нужном порядке (например, А, Б, В, Г).

10. Установите правильную последовательность действий компании при обнаружении утечки персональных данных:

А) Уведомление пострадавших клиентов

Б) Расследование причин утечки

В) Немедленное прекращение утечки

Г) Уведомление уполномоченного органа (Роскомнадзор)

Д) Внедрение мер по предотвращению повторных инцидентов

11. Установите правильную последовательность этапов внедрения системы информационной безопасности:

А) Анализ угроз и уязвимостей

Б) Внедрение выбранных средств защиты

В) Оценка текущего уровня защищенности

Г) Выбор программно-аппаратных средств защиты

Д) Мониторинг и корректировка системы

Задание открытого типа с развернутым ответом

Прочитайте текст задания, проанализируйте предложенную ситуацию. Дайте развернутый обоснованный ответ.

12. Интернет-магазин «ТехноМир» обнаружил в открытом доступе на теневом форуме базу данных клиентов (50 000 записей: ФИО, телефоны, email, адреса). В штате нет специалиста по информационной безопасности. Компания никогда не разрабатывала политику обработки персональных данных.

Вопросы:

1. Какие требования Федерального закона № 152-ФЗ нарушила компания? (Перечислите не менее 3 нарушений).

2. В какие сроки и какие органы компания обязана уведомить об утечке?

3. Разработайте текст уведомления для пострадавших клиентов.

4. Какие меры должна предпринять компания для предотвращения подобных инцидентов в будущем? (Не менее 4 мер).

КТ — 3. Раздел 3 (темы 3.1, 3.2)

Задание закрытого типа с выбором одного правильного ответа

Прочитайте текст задания, выберите один правильный ответ из предложенных вариантов. Запишите букву выбранного варианта ответа.

1. Для чего предназначены антивирусные программы?

А) для создания презентаций

Б) для обнаружения и удаления вредоносного программного обеспечения

В) для мониторинга социальных сетей

Г) для управления репутацией

2. Что такое VPN?

А) антивирусная программа

Б) технология, создающая зашифрованное соединение

В) программное обеспечение для управления проектами

Г) система мониторинга социальных сетей

3. Какой показатель НЕ относится к KPI управления цифровой репутацией?

А) рост доли позитивных упоминаний

Б) увеличение количества подписчиков в социальных сетях

В) количество внутренних приказов

Г) снижение времени реакции на негатив

4. Что из перечисленного должно входить в регламент работы с репутационными рисками?

А) порядок действий при выявлении негатива

Б) рецепты блюд в столовой

В) расписание отпусков сотрудников

Г) технические характеристики продукции

5. Что относится к средствам многофакторной аутентификации?

А) только пароль

Б) пароль + код из SMS

В) только биометрические данные

Г) только push-уведомление

Задание закрытого типа на установление соответствия

Прочитайте текст задания. Сопоставьте элементы списка 1 с элементами списка 2, сформируйте пары элементов. Запишите попарно буквы и цифры (например, А1, Б2).

6. Установите соответствие между элементов стратегии и его содержанием:

Список 1 (Элемент стратегии)	Список 2 (Содержание)
А) Цели управления репутацией	1) Увеличение доли позитивных упоминаний до 80% за год
Б) KPI	2) Мониторинг упоминаний, работа с отзывами, антикризисные коммуникации
В) Целевые показатели	3) Рост Share of Voice, снижение времени реакции на негатив
Г) Мероприятия	4) Достижение лидерства по репутации в своей нише

7. Установите соответствие между средством защиты информации и его характеристикой:

Список 1 (Средство защиты)	Список 2 (Характеристика)
А) Антивирус	1) Защита от утечек конфиденциальной информации
Б) DLP-система	2) Обнаружение и блокировка вредоносного ПО
В) VPN	3) Зашифрованное соединение с сетью Интернет
Г) Межсетевой экран	4) Фильтрация сетевого трафика по заданным правилам

Задание закрытого типа с выбором нескольких правильных ответов

Прочитайте текст задания, выберите несколько правильных ответов из предложенных вариантов. Запишите буквы выбранных вариантов ответа (например, А, Б, В).

8. Какие элементы должны входить в интегрированную стратегию управления цифровой репутацией и информационной безопасностью? (Выберите несколько)

А) цели и KPI управления репутацией

Б) перечень блюд в корпоративной столовой

В) регламенты работы с репутационными рисками и информационными угрозами

Г) план обучения сотрудников правилам цифровой гигиены

Д) график отпусков сотрудников

9. Какие методы могут использоваться для оценки эффективности управления цифровой репутацией? (Выберите несколько)

А) анализ динамики тональности упоминаний

Б) опросы удовлетворенности клиентов

В) измерение количества выпущенных внутренних приказов

Г) мониторинг Share of Voice

Д) анализ времени реакции на негативные публикации

Задание закрытого типа на установление последовательности

Прочитайте текст задания. Постройте верную последовательность из предложенных элементов. Запишите буквы в нужном порядке (например, А, Б, В, Г).

10. Установите правильную последовательность этапов разработки интегрированной стратегии управления цифровой репутацией:

А) Разработка регламентов работы с рисками

Б) Анализ текущего состояния репутации и угроз ИБ

В) Определение целей и KPI

Г) Выбор программных средств мониторинга и защиты

Д) Внедрение и корректировка стратегии

11. Установите правильную последовательность этапов внедрения DLP-системы в компании:

А) Определение критичных данных и каналов утечки

Б) Настройка политик безопасности

В) Анализ бизнес-процессов

Г) Внедрение и тестирование

Д) Обучение сотрудников

Задание открытого типа с развернутым ответом

Прочитайте текст задания, проанализируйте предложенную ситуацию. Дайте развернутый обоснованный ответ.

12. Стартап «ФитнесТрек» создает мобильное приложение для отслеживания физической активности, питания и здоровья. Приложение собирает персональные данные пользователей (вес, рост, пульс, геолокацию тренировок). Бюджет ограничен. Через 3 месяца планируется привлечение инвестиций.

Вопросы:

1. Разработайте стратегию управления цифровой репутацией для стартапа на первый год (цели, KPI, ключевые мероприятия).

2. Какие программные средства и организационные меры необходимо внедрить для обеспечения информационной безопасности с учетом ограниченного бюджета? (Минимальный набор).

3. Разработайте концепцию «страницы доверия» (Trust Center) для сайта приложения. Какие разделы она должна содержать?

4. Подготовьте краткое обоснование для инвестора (3-5 пунктов), почему управление цифровой репутацией и информационной безопасностью критически важно для успеха стартапа.

Критерии оценивания заданий в рамках контрольных точек

Критерии оценивания тестовых заданий:

Баллы	Описание критерия	
4-5	90-100% правильных ответов.	Обучающийся демонстрирует глубокое познание в освоенном материале.
3-4	60-89% правильных ответов.	Обучающимся материал освоен полностью, без существенных ошибок.
2-3	26 - 59% правильных ответов.	Обучающимся материал освоен не полностью, имеются значительные пробелы в знаниях.
0-1	0 - 25% правильных ответов.	Обучающимся материал не освоен, знания обучающегося ниже базового уровня.

0* - в журнал академической группы не выставляется

Критерии оценивания практических заданий:

Баллы	КРИТЕРИИ ОЦЕНИВАНИЯ
4-5	Полный, развернутый ответ, глубокое знание, практические задания без ошибок
2-3	Развернутый ответ, небольшие неточности, практические задания с мелкими ошибками
0-1	Ответ недостаточно полный, слабая аргументация, ошибки в практических заданиях

5.5. Описание дополнительных материалов и оборудования, необходимых для выполнения заданий.

Для выполнения проверочных заданий по дисциплине «Управление цифровой репутацией и информационная безопасность» обучающимся могут потребоваться следующие дополнительными материалы и оборудование:

1. Для выполнения практических заданий по мониторингу и анализу цифровой репутации студенту разрешается использование персонального компьютера или ноутбука с доступом к сети «Интернет».

2. Для выполнения заданий по анализу систем мониторинга цифровой репутации студенту разрешается использование демо-версий или открытых данных сервисов Brand Analytics, IQBuzz, YouScan, Медиалогия (по указанию преподавателя) или изучение интерфейсов по скриншотам и видео-обзорам.

3. Для выполнения заданий, связанных с анализом правовых норм и нормативно-правовых актов студенту разрешается использование текстов Федеральных законов:

Федеральный закон «Об информации, информационных технологиях и о защите информации»;

Федеральный закон «О персональных данных» (№ 152-ФЗ);

Кодекс Российской Федерации об административных правонарушениях (КоАП РФ);

Уголовный кодекс Российской Федерации (УК РФ).

4. Для выполнения заданий по анализу и разработке регламентов, политик и стратегий студенту разрешается использование шаблонов документов и образцов, предоставленных преподавателем.

5. Для выполнения расчетов показателей эффективности мероприятий по управлению репутацией (KPI, ROMI, охват, тональность и др.) студенту разрешается использование калькулятора (как физического, так и программного на компьютере или смартфоне).

6. При выполнении тестовых заданий закрытого типа (в рамках контрольных точек) использование дополнительных материалов и оборудования не требуется.

7. Для выполнения заданий, связанных с анализом фишинговых писем и угроз информационной безопасности, студенту разрешается использование учебных примеров и образцов, предоставленных преподавателем.

8. Для выполнения заданий по разработке памяток и чек-листов студенту разрешается использование текстовых редакторов (Microsoft Word, LibreOffice Writer, отечественные офисные пакеты) для оформления результатов.

9. Для выполнения заданий по анализу кейсов антикризисных коммуникаций студенту разрешается использование технических средств воспроизведения видео

(компьютер, ноутбук, смартфон) для просмотра учебных видеоматериалов, предоставленных преподавателем.

6. Формы промежуточной аттестации, критерии и шкала оценивания, типовые оценочные материалы по дисциплине

6.1. Форма промежуточной аттестации

Промежуточная аттестация по дисциплине «Управление цифровой репутацией и информационная безопасность» проводится в форме *зачета.*

6.2. Типовые оценочные материалы промежуточной аттестации

Типовые проверочные задания для самоподготовки обучающегося к промежуточной аттестации:

Тема 1.1. Цифровая репутация как нематериальный актив компании (УК-2.4)

Вопросы открытого типа:

1. Что такое цифровая репутация? Каковы ее основные компоненты?
2. Как цифровая репутация влияет на финансовые показатели компании?
3. Какие факторы формируют цифровую репутацию?
4. Какие нормы профессиональной этики необходимо соблюдать при работе с цифровой информацией о конкурентах?

Тестовые задания:

Внимательно прочитайте текст задания и выберите один правильный ответ из предложенных вариантов. Запишите букву выбранного варианта ответа.

1. Что из перечисленного является фактором, формирующим цифровую репутацию?

А) цветовая гамма логотипа

Б) расписание работы офиса

В) отзывы клиентов на маркетплейсах

Г) количество сотрудников в штате

2. Какой показатель отражает долю упоминаний компании в общем объеме упоминаний всех игроков рынка?

А) охват

Б) тональность

В) Share of Voice

Г) индекс репутации

Тема 1.2. Инструменты мониторинга и анализа цифровой репутации (ОПК-5.1, ОПК-6.1)

Вопросы открытого типа:

1. Какие системы мониторинга цифровой репутации существуют на российском рынке?
2. Каковы принципы работы систем мониторинга социальных медиа и СМИ?
3. Какие метрики используются для оценки цифровой репутации?
4. Что такое тональность упоминаний и как она определяется?

Тестовые задания:

Внимательно прочитайте текст задания и выберите один правильный ответ

из предложенных вариантов. Запишите букву выбранного варианта ответа.

1. Какой сервис предназначен для мониторинга и анализа цифровой репутации?

А) PowerPoint

Б) Brand Analytics

В) Excel

Г) 1С:Бухгалтерия

2. Что показывает метрика «охват» (reach)?

А) количество упоминаний компании

Б) количество уникальных пользователей, увидевших упоминание

В) долю упоминаний компании на рынке

Г) соотношение позитивных и негативных отзывов

3. Что такое «индекс репутации»?

А) количество подписчиков в социальных сетях

Б) интегральный показатель, учитывающий различные параметры репутации

В) количество упоминаний в СМИ за месяц

Г) цена акций компании

Тема 1.3. Управление репутацией в социальных медиа (SERM) (УК-2.4, ОПК-5.1)

Вопросы открытого типа:

1. Что такое SERM (Search Engine Reputation Management) и SMM-репутация?
2. Какие каналы и площадки наиболее важны для управления цифровой репутацией?
3. Как работать с отзывами на маркетплейсах?
4. Какие существуют стратегии работы с негативными отзывами?

Тестовые задания:

Внимательно прочитайте текст задания и выберите один правильный ответ из предложенных вариантов. Запишите букву выбранного варианта ответа.

1. Что означает аббревиатура SERM?

А) управление репутацией в поисковых системах

Б) управление продажами в социальных сетях

В) управление персоналом компании

Г) управление бюджетом маркетинга

2. Какая стратегия работы с негативным отзывом предполагает отсутствие публичной реакции, если отзыв необоснованный?

А) удаление

Б) эскалация

В) игнорирование

Г) публичный ответ

3. Что из перечисленного относится к инструментам управления отзывами?

А) CRM для репутации

Б) ERP-система

В) текстовый редактор

Г) графический редактор

Тема 1.4. Работа с негативом и кризисные коммуникации в цифровой среде

(УК-2.4)

Вопросы открытого типа:

1. Какие виды репутационных рисков и угроз существуют в цифровой среде?
2. Что такое информационная атака? Приведите примеры.
3. Каков алгоритм антикризисных коммуникаций?
4. Какие стратегии ответа на негатив могут быть использованы в кризисной ситуации?

Тестовые задания:

Внимательно прочитайте текст задания и выберите один правильный ответ из предложенных вариантов. Запишите букву выбранного варианта ответа.

1. Что из перечисленного является информационной атакой?

А) позитивный отзыв клиента

Б) хейтерская кампания

В) новость о запуске продукта

Г) исследование рынка

2. Что является первым этапом антикризисных коммуникаций?

А) выбор стратегии ответа

Б) публичное заявление

В) мониторинг и раннее обнаружение кризиса

Г) оценка ущерба

3. Какой метод работы с негативом предполагает удаление контента (если это не запрещено правилами площадки)?

А) игнорирование

Б) удаление

В) публичный ответ

Г) юридические меры

Тема 2.1. Правовые и этические аспекты управления цифровой репутацией (УК-2.4)

Вопросы открытого типа:

1. Какие правовые нормы регулируют работу с информацией в сети «Интернет»?
2. Что такое «право на забвение» и какова процедура удаления недостоверной информации?
3. Какая ответственность предусмотрена за клевету и оскорбления в сети «Интернет»?
4. Какие этические дилеммы возникают при управлении цифровой репутацией?

Тестовые задания:

Внимательно прочитайте текст задания и выберите один правильный ответ из предложенных вариантов. Запишите букву выбранного варианта ответа.

1. Какой Федеральный закон является основным в сфере регулирования информации в сети «Интернет»?

А) Федеральный закон «О рекламе»

Б) Федеральный закон «Об информации, информационных технологиях и о защите информации»

В) Федеральный закон «О защите прав потребителей»

Г) Федеральный закон «О конкуренции»

2. Что такое «право на забвение»?

А) право компании удалить любой негативный отзыв

Б) право гражданина требовать удаления недостоверной информации о себе из поисковых систем

В) право маркетолога игнорировать запросы клиентов

Г) право СМИ не раскрывать источники информации

3. Какая статья КоАП РФ предусматривает ответственность за оскорбление в сети «Интернет»?

А) 1.1

Б) 5.61

В) 10.5

Г) 13.15

Тема 2.2. Основы информационной безопасности для маркетолога (ОПК-5.1, ОПК-6.1)

Вопросы открытого типа:

1. Каковы основные угрозы информационной безопасности в маркетинговой деятельности?

2. Что такое фишинг и социальная инженерия? Приведите примеры.

3. Какие существуют виды средств защиты информации?

4. Что такое политика безопасности при работе с корпоративной информацией?

Тестовые задания:

Внимательно прочитайте текст задания и выберите один правильный ответ из предложенных вариантов. Запишите букву выбранного варианта ответа.

1. Что из перечисленного относится к базовым понятиям информационной безопасности?

А) конфиденциальность, целостность, доступность

Б) скорость, точность, надежность

В) качество, количество, стоимость

Г) дизайн, эргономика, стиль

2. Что такое фишинг?

А) вид компьютерного вируса

Б) вид мошенничества с целью получения конфиденциальных данных

В) метод защиты информации

Г) антивирусная программа

3. Для чего используются DLP-системы?

А) для создания презентаций

Б) для предотвращения утечек конфиденциальных данных

В) для мониторинга социальных сетей

Г) для управления репутацией

Тема 2.3. Защита персональных данных в маркетинговой деятельности (УК-2.4, ОПК-6.1)

Вопросы открытого типа:

1. Что такое персональные данные согласно Федеральному закону № 152-ФЗ?

2. Какие требования предъявляются к сбору, хранению, обработке и передаче персональных данных?

3. Что должно содержать согласие на обработку персональных данных?

4. Какие права имеют субъекты персональных данных?

Тестовые задания:

Внимательно прочитайте текст задания и выберите один правильный ответ из предложенных вариантов. Запишите букву выбранного варианта ответа.

1. Какой Федеральный закон регулирует вопросы обработки персональных данных?

А) № 38-ФЗ «О рекламе»

Б) № 152-ФЗ «О персональных данных»

В) № 149-ФЗ «Об информации...»

Г) № 135-ФЗ «О защите конкуренции»

2. Что из перечисленного НЕ относится к персональным данным?

А) фамилия, имя, отчество

Б) дата и место рождения

В) ИНН компании

Г) адрес места жительства

3. Что должно содержать согласие на обработку персональных данных?

А) только подпись субъекта

Б) цель обработки, перечень данных, срок действия, подпись

В) только перечень данных

Г) только срок действия согласия

Тема 3.1. Программные средства для обеспечения информационной безопасности (ОПК-5.1, ОПК-6.1)

Вопросы открытого типа:

1. Какие классы программных средств для обеспечения информационной безопасности вы знаете?

2. Какие задачи решают антивирусные решения? Назовите примеры.

3. Для чего используются средства шифрования данных?

4. Что такое многофакторная аутентификация и как она работает?

Тестовые задания:

Внимательно прочитайте текст задания и выберите один правильный ответ из предложенных вариантов. Запишите букву выбранного варианта ответа.

1. Для чего предназначены антивирусные программы?

А) для создания презентаций

Б) для обнаружения и удаления вредоносного программного обеспечения

В) для мониторинга социальных сетей

Г) для управления репутацией

2. Что такое VPN?

А) антивирусная программа

Б) технология, создающая зашифрованное соединение между устройством и сетью

В) программное обеспечение для управления проектами

Г) система мониторинга социальных сетей

3. Что относится к средствам многофакторной аутентификации?

А) только пароль

Б) пароль + код из SMS

В) только биометрические данные

Г) только push-уведомление

Тема 3.2. Интегрированная стратегия управления цифровой репутацией и информационной безопасностью (УК-2.4, ОПК-5.1, ОПК-6.1)

Вопросы открытого типа:

1. Как разработать стратегию управления цифровой репутацией компании? Какие элементы она включает?

2. Какие KPI и целевые показатели используются для оценки эффективности управления репутацией?

3. Как интегрировать управление репутацией с информационной безопасностью и маркетинговой стратегией?

4. Как обучить сотрудников правилам цифровой гигиены и репутационной безопасности?

Тестовые задания:

Внимательно прочитайте текст задания и выберите один правильный ответ из предложенных вариантов. Запишите букву выбранного варианта ответа.

1. Какой показатель НЕ относится к KPI управления цифровой репутацией?

А) рост доли позитивных упоминаний

Б) увеличение количества подписчиков в социальных сетях

В) количество внутренних приказов

Г) снижение времени реакции на негатив

2. Что из перечисленного должно входить в регламент работы с репутационными рисками?

А) порядок действий при выявлении негатива

Б) рецепты блюд в столовой

В) расписание отпусков сотрудников

Г) технические характеристики продукции

3. Как часто рекомендуется пересматривать стратегию управления цифровой репутацией?

А) один раз в 10 лет

Б) регулярно, с учетом изменения правовых и этических требований

В) только при смене руководителя

Г) никогда

Тестовые задания комбинированного типа

Внимательно прочитайте текст задания, выберите один правильный ответ из предложенных вариантов. Запишите букву выбранного варианта ответа, а также обоснуйте ваш выбор.

Задание 1. Компания обнаружила в социальных сетях фейковый негативный отзыв о своей продукции. Какое действие будет наиболее правильным в данной ситуации?

А) удалить отзыв через администрацию платформы (если это предусмотрено правилами)

Б) проигнорировать отзыв

В) публично ответить с опровержением и доказательствами

Г) написать несколько фейковых позитивных отзывов

Ключ правильного ответа: А или В (в зависимости от конкретной ситуации и правил платформы). Обоснование: удаление возможно, если отзыв нарушает правила платформы (оскорбления, ложная информация). Публичный ответ с опровержением также допустим, если компания может предоставить доказательства. Игнорирование может привести к распространению ложной информации, а написание фейковых отзывов является нарушением профессиональной этики.

Задание 2. Компания собирает персональные данные клиентов через форму подписки на новостную рассылку. Какое требование Федерального закона № 152-ФЗ является обязательным?

А) согласие на обработку персональных данных должно быть получено в письменной форме на бумажном носителе

Б) согласие должно содержать цель обработки, перечень данных, срок действия и подпись (или отметка в электронной форме)

В) согласие требуется только для передачи данных третьим лицам

Г) согласие не требуется, если данные собираются через форму на сайте

Ключ правильного ответа: Б. Обоснование: согласно ст. 9 Федерального закона № 152-ФЗ, согласие должно быть конкретным, информированным и сознательным, а также содержать цель обработки, перечень персональных данных, срок действия согласия и способ его подтверждения (подпись, галочка в чек-боксе и т.д.).

6.3. Критерии и шкала оценивания на основе БРС.

КРИТЕРИИ ОЦЕНИВАНИЯ	РЕЗУЛЬТАТ В БАЛЛАХ
Дан полный, в логической последовательности развернутый ответ на поставленный вопрос, где он продемонстрировал знания предмета в полном объеме учебной программы, достаточно глубоко осмысливает дисциплину, самостоятельно, и исчерпывающе отвечает на дополнительные вопросы, приводит собственные примеры по проблематике поставленного вопроса, решил предложенные практические задания без ошибок	90-100
Дан развернутый ответ на поставленный вопрос, где обучающийся демонстрирует знания, приобретенные на лекционных и семинарских занятиях, а также полученные посредством изучения обязательных учебных материалов по курсу, дает аргументированные ответы, приводит примеры, в ответе присутствует свободное владение монологической речью, логичность и последовательность ответа. Однако допускается неточность в ответе. Решил предложенные практические задания с небольшими неточностями.	75-89
Дан ответ, свидетельствующий в основном о знании процессов изучаемой дисциплины, отличающийся недостаточной глубиной и полнотой раскрытия темы, знанием основных вопросов теории, слабо сформированными навыками анализа явлений, процессов, недостаточным умением давать	60-74

аргументированные ответы и приводить примеры, недостаточно свободным владением монологической речью, логичностью и последовательностью ответа. Допускается несколько ошибок в содержании ответа и решении практических заданий.	
Дан ответ, который содержит ряд серьезных неточностей, обнаруживающий незнание процессов изучаемой предметной области, отличающийся неглубоким раскрытием темы, незнанием основных вопросов теории, несформированными навыками анализа явлений, процессов, неумением давать аргументированные ответы, слабым владением монологической речью, отсутствием логичности и последовательности. Выводы поверхностны. Решение практических заданий не выполнено, т.е. обучающийся не способен ответить на вопросы даже при дополнительных наводящих вопросах преподавателя.	1-59

7. Методические материалы по освоению дисциплины (модуля)

Подготовка к лекциям.

Главное в период подготовки к лекционным занятиям – научиться методам самостоятельного умственного труда, сознательно развивать свои творческие способности и овладевать навыками творческой работы. Для этого необходимо строго соблюдать дисциплину учебы и поведения. Четкое планирование своего рабочего времени и отдыха является необходимым условием для успешной самостоятельной работы. В основу его нужно положить рабочие программы изучаемых в семестре дисциплин. Каждому обучающемуся следует составлять еженедельный и семестровый планы работы, а также план на каждый рабочий день. С вечера всегда надо распределять работу на завтрашний день. В конце каждого дня целесообразно подводить итог работы: тщательно проверить, все ли выполнено по намеченному плану, не было ли каких-либо отступлений, а если были, по какой причине это произошло. Нужно осуществлять самоконтроль, который является необходимым условием успешной учебы. Если что-то осталось невыполненным, необходимо изыскать время для завершения этой части работы, не уменьшая объема недельного плана.

Самостоятельная работа на лекции.

Слушание и запись лекций – сложный вид вузовской аудиторной работы. Внимательное слушание и конспектирование лекций предполагает интенсивную умственную деятельность обучающегося. Краткие записи лекций, их конспектирование помогает усвоить учебный материал. Конспект является полезным тогда, когда записано самое существенное, основное и сделано это самим обучающимся. Не надо стремиться записать дословно всю лекцию. Такое «конспектирование» приносит больше вреда, чем пользы. Запись лекций рекомендуется вести по возможности собственными формулировками. Желательно запись осуществлять на одной странице, а следующую оставлять для проработки учебного материала самостоятельно в домашних условиях. Конспект лекции лучше подразделять на пункты, параграфы, соблюдая красную строку. Этому в большой

степени будут способствовать пункты плана лекции, предложенные преподавателям. Принципиальные места, определения, формулы и другое следует сопровождать замечаниями «важно», «особо важно», «хорошо запомнить» и т.п. Можно делать это и с помощью разноцветных маркеров или ручек. Лучше если они будут собственными, чтобы не приходилось просить их у однокурсников и тем самым не отвлекать их во время лекции. Целесообразно разработать собственную «маркографию» (значки, символы), сокращения слов. Не лишним будет и изучение основ стенографии. Работая над конспектом лекций, всегда необходимо использовать не только учебник, но и ту литературу, которую дополнительно рекомендовал лектор. Именно такая серьезная, кропотливая работа с лекционным материалом позволит глубоко овладеть знаниями.

Подготовка к практическим занятиям.

Подготовку к каждому практическому занятию каждый обучающийся должен начать с ознакомления с планом практического занятия, который отражает содержание предложенной темы. Тщательное продумывание и изучение вопросов плана основывается на проработке текущего материала лекции, а затем изучения обязательной и дополнительной литературы, рекомендованную к данной теме. На основе индивидуальных предпочтений обучающемуся необходимо самостоятельно выбрать тему доклада по проблеме практического занятия и по возможности подготовить по нему презентацию. Если программой дисциплины предусмотрено выполнение практического задания, то его необходимо выполнить с учетом предложенной инструкции (устно или письменно). Все новые понятия по изучаемой теме необходимо выучить наизусть и внести в глоссарий, который целесообразно вести с самого начала изучения курса. Результат такой работы должен проявиться в способности обучающегося свободно ответить на теоретические вопросы практического занятия, его выступлении и участии в коллективном обсуждении вопросов изучаемой темы, правильном выполнении практических заданий и контрольных работ.

Работа с литературными источниками.

В процессе подготовки к практическим занятиям, обучающимся необходимо обратить особое внимание на самостоятельное изучение рекомендованной учебно-методической (а также научной и популярной) литературы. Самостоятельная работа с учебниками, учебными пособиями, научной, справочной и популярной литературой, материалами периодических изданий и Интернета, статистическими данными является наиболее эффективным методом получения знаний, позволяет значительно активизировать процесс овладения информацией, способствует более глубокому усвоению изучаемого материала, формирует у обучающихся свое отношение к конкретной проблеме. Более глубокому раскрытию вопросов способствует знакомство с дополнительной литературой, рекомендованной преподавателем, что позволяет обучающимся проявить свою индивидуальность в рамках выступления на занятиях, выявить широкий спектр мнений по изучаемой проблеме.

8. Учебная литература и ресурсы информационно- телекоммуникационной сети Интернет

8.1. Основная литература

1. Чумиков, А.Н. Реклама и связи с общественностью: имидж, репутация, бренд : учеб. пособие для студентов вузов / А.Н. Чумиков. — 2-е изд., испр. и доп. — Москва : Аспект Пресс, 2016. — 159 с. — (Учебник нового поколения). - ISBN 978-5-7567-0819-6. - Текст : электронный. - URL: https://znanium.ru/catalog/product/1039478 (дата обращения: 02.05.2026). – Режим доступа: по подписке.

2. Бюрг, Ю. Формула онлайн-репутации, или Простыми словами об ORM : практическое руководство / Ю. Бюрг, О. Кошкин. - Москва : Альпина ПРО, 2026. - 272 с. - ISBN 978-5-206-00012-2. - Текст : электронный. - URL: https://znanium.ru/catalog/product/2236051 (дата обращения: 02.05.2026). – Режим доступа: по подписке.

3. Рева, В. Е. Управление репутацией : учебное пособие / В. Е. Рева. - 3-е изд., стер. - Москва : Дашков и К, 2022. - 136 с. - ISBN 978-5-394-04616-2. - Текст : электронный. - URL: https://znanium.com/catalog/product/2084841 (дата обращения: 02.05.2026). – Режим доступа: по подписке.

4. Козлова, Н.П. Особенности формирования деловой репутации современной компании: Монография / Н. П. Козлова. — Москва : Издательско-торговая корпорация «Дашков и К°», 2014. — 376 с. - ISBN 978-5-394-02437-5 -. - Текст : электронный. - URL: https://znanium.com/catalog/product/514171 (дата обращения: 02.05.2026). – Режим доступа: по подписке.

5. Клименко, И. С. Информационная безопасность и защита информации: модели и методы управления : монография / И.С. Клименко. — Москва : ИНФРА-М, 2021. — 180 с. — (Научная мысль). — DOI 10.12737/monography_5d412ff13c0b88.75804464. - ISBN 978-5-16-015149-6. - Текст : электронный. - URL: https://znanium.ru/catalog/product/1137902 (дата обращения: 02.05.2026)

6. Бирюков, А. А. Информационная безопасность: защита и нападение : практическое руководство / А. А. Бирюков. - Москва : ДМК Пресс, 2017. - 436 с. - ISBN 978-5-97060-435-9. - Текст : электронный. - URL: https://znanium.ru/catalog/product/1908424 (дата обращения: 02.05.2026). – Режим доступа: по подписке.

8.2. Дополнительная литература

1. Шарков, Ф. И. Константы гудвилла: стиль, паблисити, репутация, имидж и бренд фирмы : учебное пособие / Ф. И. Шарков. - 5-е изд., стер. - Москва : Издательско-торговая корпорация «Дашков и К°», 2020. — 270 с. - ISBN 978-5-394-03640-8. - Текст : электронный. - URL: https://znanium.com/catalog/product/1093679 (дата обращения: 02.05.2026). – Режим доступа: по подписке.

2. Домбай, К. Конец пиара : Управление репутацией как финансовым капиталом : практическое руководство / К. Домбай. - Москва : Альпина ПРО, 2026. - 96 с. - ISBN 978-5-206-00174-7. - Текст : электронный. - URL: https://znanium.ru/catalog/product/2236324 (дата обращения: 02.05.2026). – Режим доступа: по подписке.

3. Гаврилов, Е. В. Компенсация нематериального (репутационного) вреда как способ защиты деловой репутации юридических лиц : монография / Е. В. Гаврилов. - Москва : Юстицинформ, 2022. - 344 с. - ISBN 978-5-7205-1786-1. - Текст : электронный. - URL: https://znanium.com/catalog/product/1859692 (дата обращения: 02.05.2026). – Режим доступа: по подписке.

4. Управление деловой репутацией : учебное пособие / С. Н. Лебедева, А. З. Коробкин, Т. П. Афонченко [и др.] ; под. ред. В. Н. Дорошко. - Минск : Вышэйшая школа, 2020. - 188 с. - ISBN 978-985-06-3194-7. - Текст : электронный. - URL: https://znanium.com/catalog/product/2131520 (дата обращения: 02.05.2026). – Режим доступа: по подписке.

5. Стулова, Е. Четыре всадника информационного апокалипсиса : Краткое пособие по управлению репутацией политика в условиях новой информационной реальности : практическое пособие / Е. Стулова. - Москва : Альпина ПРО, 2026. - 96 с. - ISBN 978-5-907470-27-9. - Текст : электронный. - URL: https://znanium.ru/catalog/product/2235795 (дата обращения: 02.05.2026). – Режим доступа: по подписке.

6. Шаньгин, В. Ф. Информационная безопасность и защита информации : учебное пособие / В. Ф. Шаньгин. - Москва : ДМК Пресс, 2017. - 703 с. - ISBN 978-5-97060-439-7. - Текст : электронный. - URL: https://znanium.ru/catalog/product/1908081 (дата обращения: 02.05.2026). – Режим доступа: по подписке.

8.3. Интернет-ресурсы

ЭБС «ЛАНЬ» - https://e.lanbook.com

ЭБС «ЗНАНИУМ» - https://znanium.ru

ЭБС «SOCHUM» - https://sochum.ru

9. Материально-техническая база, информационные технологии, программное обеспечение и информационные справочные системы

Требования к аудитории:

- Лекционные
- Семинарские
- Помещения для самостоятельной работы

Требования к оборудованию:

- Доска
- проектор
- ПК (стационарный) или ноутбук: операционная система: не ниже Windows 7 (или аналогичная по функциям)

Требования к программному обеспечению:

- пакет Microsoft Office