

МИНИСТЕРСТВО ПРОСВЕЩЕНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ  
федеральное государственное бюджетное образовательное учреждение высшего  
образования  
«Красноярский государственный педагогический университет  
им. В.П. Астафьева»  
(КГПУ им. В.П. Астафьева)

## МОДУЛЬ 1 "МЕТОДОЛОГИЯ ИССЛЕДОВАНИЯ В ПСИХОЛОГИИ" Информационная культура профильной организации

### рабочая программа дисциплины (модуля)

Закреплена за кафедрой

D8 Информатики и информационных технологий в образовании

Учебный план

37.04.01 Психологическое консультирование и психотерапия (о, 2025).plx  
Направление поготовки 37.04.01 Психология  
Направленность (профиль) образовательной программы  
Психологическое консультирование и психотерапия

Квалификация

**магистр**

Форма обучения

**очная**

Общая трудоемкость

**4 ЗЕТ**

Часов по учебному плану

144

Виды контроля в семестрах:

в том числе:

зачеты 1

аудиторные занятия 12

самостоятельная работа 131,85

контактная работа во время  
промежуточной аттестации (ИКР) 0

#### Распределение часов дисциплины по семестрам

Семестр (<Курс>.<Семестр на курсе>)	1 (1.1)		Итого	
	Недель	17 2/6		
Вид занятий	УП	РП	УП	РП
Лекции	4	4	4	4
Практические	8	8	8	8
Контроль на промежуточную аттестацию (экзамен)	0,15	0,15	0,15	0,15
Итого ауд.	12	12	12	12
Контактная работа	12,15	12,15	12,15	12,15
Сам. работа	131,85	131,85	131,85	131,85
Итого	144	144	144	144

Программу составил(и):  
кпп, Доцент, Ломаско П.С. \_\_\_\_\_

Рабочая программа дисциплины  
**Информационная культура профильной организации**

разработана в соответствии с ФГОС ВО:

Федеральный государственный образовательный стандарт высшего образования - магистратура по направлению подготовки 37.04.01 Психология (приказ Минобрнауки России от 29.07.2020 г. № 841)

составлена на основании учебного плана:

Направление подготовки 37.04.01 Психология

Направленность (профиль) образовательной программы

Психологическое консультирование и психотерапия

утвержденного учёным советом вуза от 25.06.2025 протокол № 8.

Рабочая программа одобрена на заседании кафедры  
**D8 Информатики и информационных технологий в образовании**

Протокол от 07.05.2025 г. № 9

Зав. кафедрой д-р пед. наук, профессор Пак Н.И.

Согласовано с представителями работодателей на заседании НМС УГН(С), протокол №\_\_\_\_ от \_\_ \_\_\_\_ 20\_\_ г.

Председатель НМС УГН(С)

\_\_\_\_ 2025 г.

## 1. ЦЕЛИ ОСВОЕНИЯ ДИСЦИПЛИНЫ (МОДУЛЯ)

формирование способности и готовности обучающихся к эффективному, ответственному и безопасному использованию современных цифровых технологий при осуществлении профессиональной деятельности в профильных организациях

## 2. МЕСТО ДИСЦИПЛИНЫ (МОДУЛЯ) В СТРУКТУРЕ ОБРАЗОВАТЕЛЬНОЙ ПРОГРАММЫ

Цикл (раздел) ОП:	B1.ОДП.01
<b>2.1 Требования к предварительной подготовке обучающегося:</b>	
2.1.1	Деловой иностранный язык
2.1.2	Методология и методы научного исследования (качественные и количественные методы)
2.1.3	Информационно-коммуникационные технологии в профессиональной деятельности психолога
<b>2.2 Дисциплины (модули) и практики, для которых освоение данной дисциплины (модуля) необходимо как предшествующее:</b>	
2.2.1	Подготовка к защите и защита выпускной квалификационной работы
2.2.2	Подготовка к сдаче и сдача государственного экзамена
2.2.3	Педагогическая практика

## 3. ФОРМИРУЕМЫЕ КОМПЕТЕНЦИИ И ИНДИКАТОРЫ ИХ ДОСТИЖЕНИЯ

**УК-3: Способен организовывать и руководить работой команды, вырабатывая командную стратегию для достижения поставленной цели**

:

**Знать:**

Уровень 1	все возможности ИКТ для того, чтобы организовывать и руководить работой команды, вырабатывая командную стратегию для достижения поставленной цели
Уровень 2	большинство возможностей ИКТ для того, чтобы организовывать и руководить работой команды, вырабатывая командную стратегию для достижения поставленной цели
Уровень 3	некоторую часть возможностей ИКТ для того, чтобы организовывать и руководить работой команды, вырабатывая командную стратегию для достижения поставленной цели

**Уметь:**

Уровень 1	полностью самостоятельно использовать средства ИКТ для того, чтобы организовывать и руководить работой команды, вырабатывая командную стратегию для достижения поставленной цели
Уровень 2	в большей степени самостоятельно использовать средства ИКТ для того, чтобы организовывать и руководить работой команды, вырабатывая командную стратегию для достижения поставленной цели
Уровень 3	с посторонней помощью использовать средства ИКТ для того, чтобы организовывать и руководить работой команды, вырабатывая командную стратегию для достижения поставленной цели

**Владеть:**

Уровень 1	всеми необходимыми ИКТ-навыками для того, чтобы организовывать и руководить работой команды, вырабатывая командную стратегию для достижения поставленной цели
Уровень 2	большинством необходимых ИКТ-навыков для того, чтобы организовывать и руководить работой команды, вырабатывая командную стратегию для достижения поставленной цели
Уровень 3	некоторой частью ИКТ-навыков для того, чтобы организовывать и руководить работой команды, вырабатывая командную стратегию для достижения поставленной цели

**УК-4: Способен применять современные коммуникативные технологии, в том числе на иностранном(ых) языке(ах), для академического и профессионального взаимодействия**

:

**Знать:**

Уровень 1	все возможности ИКТ для того, чтобы применять современные коммуникативные технологии, в том числе на иностранном(ых) языке(ах), для академического и профессионального взаимодействия
Уровень 2	полностью самостоятельно использовать средства ИКТ для того, чтобы применять современные коммуникативные технологии, в том числе на иностранном(ых) языке(ах), для академического и профессионального взаимодействия

Уровень 3	некоторую часть возможностей ИКТ для того, чтобы применять современные коммуникативные технологии, в том числе на иностранном(ых) языке(ах), для академического и профессионального взаимодействия
<b>Уметь:</b>	
Уровень 1	полностью самостоятельно использовать средства ИКТ для того, чтобы применять современные коммуникативные технологии, в том числе на иностранном(ых) языке(ах), для академического и профессионального взаимодействия
Уровень 2	в большей степени самостоятельно использовать средства ИКТ для того, чтобы применять современные коммуникативные технологии, в том числе на иностранном(ых) языке(ах), для академического и профессионального взаимодействия
Уровень 3	с посторонней помощью использовать средства ИКТ для того, чтобы применять современные коммуникативные технологии, в том числе на иностранном(ых) языке(ах), для академического и профессионального взаимодействия
<b>Владеть:</b>	
Уровень 1	всеми необходимыми ИКТ-навыками для того, чтобы применять современные коммуникативные технологии, в том числе на иностранном(ых) языке(ах), для академического и профессионального взаимодействия
Уровень 2	большинством необходимых ИКТ-навыков для того, чтобы применять современные коммуникативные технологии, в том числе на иностранном(ых) языке(ах), для академического и профессионального взаимодействия
Уровень 3	некоторой частью ИКТ-навыков для того, чтобы применять современные коммуникативные технологии, в том числе на иностранном(ых) языке(ах), для академического и профессионального взаимодействия
<b>УК-5: Способен анализировать и учитывать разнообразие культур в процессе межкультурного взаимодействия</b>	
:	
<b>Знать:</b>	
Уровень 1	все возможности ИКТ для того, чтобы анализировать и учитывать разнообразие культур в процессе межкультурного взаимодействия
Уровень 2	большинство возможностей ИКТ для того, чтобы анализировать и учитывать разнообразие культур в процессе межкультурного взаимодействия
Уровень 3	некоторую часть возможностей ИКТ для того, чтобы анализировать и учитывать разнообразие культур в процессе межкультурного взаимодействия
<b>Уметь:</b>	
Уровень 1	полностью самостоятельно использовать средства ИКТ для того, чтобы анализировать и учитывать разнообразие культур в процессе межкультурного взаимодействия
Уровень 2	в большей степени самостоятельно использовать средства ИКТ для того, чтобы анализировать и учитывать разнообразие культур в процессе межкультурного взаимодействия
Уровень 3	с посторонней помощью использовать средства ИКТ для того, чтобы анализировать и учитывать разнообразие культур в процессе межкультурного взаимодействия
<b>Владеть:</b>	
Уровень 1	всеми необходимыми ИКТ-навыками для того, чтобы анализировать и учитывать разнообразие культур в процессе межкультурного взаимодействия
Уровень 2	большинством необходимых ИКТ-навыков для того, чтобы анализировать и учитывать разнообразие культур в процессе межкультурного взаимодействия
Уровень 3	некоторой частью ИКТ-навыков для того, чтобы анализировать и учитывать разнообразие культур в процессе межкультурного взаимодействия
<b>ПК-1: Готов модифицировать, адаптировать существующие и создавать новые методы и методики научно-исследовательской и практической деятельности в определенной области психологии с использованием современных информационных технологий</b>	
:	
<b>Знать:</b>	
Уровень 1	все возможности ИКТ для того, чтобы модифицировать, адаптировать существующие и создавать новые методы и методики научно-исследовательской и практической деятельности в определенной области психологии
Уровень 2	большинство возможностей ИКТ для того, чтобы модифицировать, адаптировать существующие и создавать новые методы и методики научно-исследовательской и практической деятельности в определенной области психологии
Уровень 3	некоторую часть возможностей ИКТ для того, чтобы модифицировать, адаптировать существующие и создавать новые методы и методики научно-исследовательской и практической деятельности в определенной области психологии

	психологии
<b>Уметь:</b>	
Уровень 1	полностью самостоятельно использовать средства ИКТ для того, чтобы модифицировать, адаптировать существующие и создавать новые методы и методики научно-исследовательской и практической деятельности в определенной области психологии
Уровень 2	в большей степени самостоятельно использовать средства ИКТ для того, чтобы модифицировать, адаптировать существующие и создавать новые методы и методики научно-исследовательской и практической деятельности в определенной области психологии
Уровень 3	с посторонней помощью использовать средства ИКТ для того, чтобы модифицировать, адаптировать существующие и создавать новые методы и методики научно-исследовательской и практической деятельности в определенной области психологии
<b>Владеть:</b>	
Уровень 1	всеми необходимыми ИКТ-навыками для того, чтобы модифицировать, адаптировать существующие и создавать новые методы и методики научно-исследовательской и практической деятельности в определенной области психологии
Уровень 2	большинством необходимых ИКТ-навыков для того, чтобы модифицировать, адаптировать существующие и создавать новые методы и методики научно-исследовательской и практической деятельности в определенной области психологии
Уровень 3	некоторой частью ИКТ-навыков для того, чтобы модифицировать, адаптировать существующие и создавать новые методы и методики научно-исследовательской и практической деятельности в определенной области психологии

#### **4. СТРУКТУРА И СОДЕРЖАНИЕ ДИСЦИПЛИНЫ (МОДУЛЯ)**

Код занятия	Наименование разделов и тем /вид занятия/	Семестр / Курс	Часов	Компетенции	Литература и эл. ресурсы	Инте ракт.	Примечание
	<b>Раздел 1. Введение в информационную культуру профильной организации</b>						
1.1	Понятие и составляющие информационной культуры человека, организации, социума. Стадии развития информационной культуры. /Ср/	1	24	УК-5 ПК-1 УК-4 УК-3	Л1.1 Л1.2 Л1.3 Л1.4 Л1.5 Л1.6 Л1.7 Л1.9 Л1.10 Л1.11Л2.1 Л2.2Л3.1 Л3.2		Изучение учебных материалов, работа с литературой, прохождение входного тестирования
	<b>Раздел 2. Составляющие информационной культуры профильной организации</b>						
2.1	Информационная культура как феномен современного этапа развития человечества /Лек/	1	2	ПК-1 УК-4 УК-3	Л1.6 Л1.9 Л1.11Л2.1 Л2.2Л3.1 Л3.2		Конспект лекции, вопросы и задания к зачету
2.2	Информационная культура как феномен современного этапа развития человечества /Ср/	1	24	УК-5 ПК-1 УК-3	Л1.5 Л1.6 Л1.9 Л1.10 Л1.11Л2.1 Л2.2Л3.1 Л3.2		Изучение дополнительных учебных материалов, работа с литературой, выполнение индивидуальных заданий

2.3	Анализ составляющих информационной культуры /Пр/	1	2	УК-5 ПК-1 УК-3	Л1.1 Л1.2 Л1.3 Л1.5 Л1.7 Л1.8 Л1.9 Л1.10 Л1.11Л2.1 Л2.2Л3.1 Л3.2		Выполнение практических заданий
2.4	Этика и легальное использование цифровых средств и ресурсов в организациях /Лек/	1	2	УК-5 ПК-1 УК-3	Л1.1 Л1.2 Л1.3 Л1.5 Л1.7 Л1.9 Л1.10 Л1.11Л2.1 Л2.2Л3.1 Л3.2		Конспект лекции, вопросы и задания к зачету
2.5	Этика и легальное использование цифровых средств и ресурсов в организациях /Ср/	1	24	УК-5 ПК-1 УК-3	Л1.1 Л1.2 Л1.3 Л1.5 Л1.7 Л1.9 Л1.10 Л1.11Л2.1 Л2.2Л3.1 Л3.2		Изучение дополнительных учебных материалов, работа с литературой, выполнение индивидуальных заданий
2.6	Нормативно-законодательные основы использования цифровых средств в профессиональной деятельности. Цифровой ethos и этикет. /Пр/	1	2	УК-5 УК-4 УК-3	Л1.1 Л1.2 Л1.5 Л1.8 Л1.9 Л1.10 Л1.11 Л1.12Л2.1 Л2.2Л3.1 Л3.2		Выполнение практических заданий
2.7	Информационная безопасность и защита информации при использовании цифровых средств в профессиональной деятельности /Пр/	1	4	УК-5 УК-4 УК-3	Л1.1 Л1.2 Л1.3 Л1.5 Л1.6 Л1.7 Л1.9 Л1.10 Л1.11Л2.1 Л2.2Л3.1 Л3.2		Выполнение практических заданий
2.8	Информационная безопасность и защита информации при использовании цифровых средств в профессиональной деятельности /Ср/	1	36	ПК-1 УК-4 УК-3	Л1.1 Л1.2 Л1.3 Л1.5 Л1.6 Л1.7 Л1.9 Л1.10 Л1.11Л2.1 Л2.2Л3.1 Л3.2		Изучение дополнительных учебных материалов, работа с литературой, выполнение индивидуальных заданий
	<b>Раздел 3. Зачет</b>						
3.1	Подготовка к зачету /Ср/	1	23,85	УК-5 ПК-1 УК-4 УК-3	Л1.1 Л1.2 Л1.3 Л1.4 Л1.5 Л1.6 Л1.7 Л1.8 Л1.9 Л1.10 Л1.11 Л1.12Л2.1 Л2.2Л3.1 Л3.2		Повторение учебных материалов, работа с литературой, выполнение заданий на зачет
3.2	Зачет /КРЭ/	1	0,15	УК-5 ПК-1 УК-4 УК-3	Л1.1 Л1.2 Л1.3 Л1.4 Л1.5 Л1.6 Л1.7 Л1.8 Л1.9 Л1.10 Л1.11 Л1.12Л2.1 Л2.2Л3.1 Л3.2		Прохождение устного собеседования на зачете

## 5. ФОНД ОЦЕНОЧНЫХ СРЕДСТВ

### 5.1. Контрольные вопросы и задания

1. Контрольные вопросы и задания для проведения входного контроля (примеры тестовых заданий)

1. Что понимается под информационной культурой в организации?

- a) Набор навыков и знаний, связанных с использованием информации и технологий в организационной среде.
- b) Умение работать с бумажными документами.
- c) Знание истории организации.
- d) Умение эффективно использовать социальные сети.

2. Какую роль играет цифровая среда в организации?

- a) Обеспечивает удобное рабочее место для сотрудников.
- b) Упрощает коммуникацию и совместную работу с использованием цифровых инструментов.
- c) Создает ограничения в доступе к информации.
- d) Позволяет снизить расходы на техническое оборудование.

3. Какие риски связаны с использованием цифровых технологий в организационной среде?

- a) Потеря конфиденциальности информации.
- b) Увеличение производительности сотрудников.
- c) Упрощение процессов принятия управленческих решений.
- d) Расширение возможностей для творческой работы.

4. Какие основные принципы информационной безопасности следует соблюдать в организации?

- a) Регулярное обновление программного обеспечения.
- b) Установка паролей на все компьютеры и устройства.
- c) Ограничение доступа к конфиденциальной информации только уполномоченным лицам.
- d) Публикация всех данных организации в открытых источниках.

5. Что означает понятие "цифровая этика"?

- a) Правила и нормы поведения в цифровой среде.
- b) Знание основ программирования.
- c) Умение использовать электронную почту.
- d) Обучение работе с офисными программами.

6. Какие меры следует предпринять для защиты информации в цифровой среде организации?

- a) Регулярное резервное копирование данных.
- b) Запрет использования любых цифровых технологий в организации.
- c) Разглашение информации организации в социальных сетях.
- d) Публикация конфиденциальных данных на общедоступных ресурсах.

7. Какую роль играет лидерство в формировании информационной культуры организации?

- a) Лидерство является ключевым элементом в формировании информационной культуры организации и должно поддерживать принципы безопасного и эффективного использования цифровых технологий.
- b) Лидерство не играет существенной роли в формировании информационной культуры организации.
- c) Лидерство ответственно за разработку цифровых технологий в организации.
- d) Лидерство несет ответственность за нарушения информационной безопасности в организации.

8. Какие навыки и знания важны для эффективного использования цифровых технологий в профессиональной деятельности?

- a) Умение проводить онлайн-трансляции и вебинары.
- b) Умение анализировать большие объемы данных.
- c) Понимание основ работы с программами обработки текста и электронными таблицами.
- d) Знание истории развития компьютеров.

9. Какие факторы могут влиять на успешное использование цифровых технологий в организации?

- a) Наличие достаточных финансовых ресурсов для приобретения необходимого оборудования.
- b) Положительная организационная культура, поддерживающая инновации и обучение сотрудников.
- c) Отсутствие необходимых технических знаний у сотрудников.
- d) Разработка и реализация стратегии внедрения цифровых технологий без учета потребностей организации.

10. Какие методы обучения и поддержки сотрудников могут быть эффективными при внедрении цифровых технологий в организации?

- a) Проведение тренингов и обучающих курсов.
- b) Создание цифровых инструкций и видеоматериалов для самостоятельного обучения.
- c) Использование мотивационных систем и наград для стимулирования использования цифровых технологий.
- d) Отказ от обучения сотрудников, так как они должны осваивать цифровые технологии самостоятельно.

**Критерии оценивания**

% верных ответов Академическая оценка

0 – 60 Не зачтено

61 – 100 Зачтено

**2. Контрольные вопросы и задания для проведения текущего контроля (примеры тестовых заданий)****1. Какие основные принципы информационной культуры должны быть соблюдены в профильной организации?**

- a) Конфиденциальность, целостность, доступность.
- b) Инновации, авторское право, этикет.
- c) Производительность, надежность, масштабируемость.
- d) Стабильность, конкурентоспособность, эффективность.

**2. Что означает соблюдение законодательства в контексте информационной культуры организации?**

- a) Соблюдение нормативных актов, касающихся обработки и защиты информации.
- b) Активное участие в разработке новых законов о цифровой среде.
- c) Использование информации без ограничений и официального разрешения.
- d) Непосредственное привлечение юристов к работе с информацией.

**3. Какие меры можно принять для защиты информации в профильной организации?**

- a) Использование паролей, шифрование данных, ограничение физического доступа.
- b) Установка брандмауэра, отключение интернета, удаление всех данных.
- c) Распространение информации без ограничений для повышения прозрачности.
- d) Использование общедоступных облачных хранилищ для всех данных.

**4. Какие нарушения цифрового этикета могут повлиять на профессиональную репутацию организации?**

- a) Некорректное использование электронной почты и социальных сетей.
- b) Отсутствие аккаунта в социальных сетях.
- c) Использование шифрования для всех персональных данных.
- d) Передача информации по электронной почте без защиты.

**5. Что означает информационная безопасность в контексте профильной организации?**

- a) Защита информации от несанкционированного доступа, использования и распространения.
- b) Открытый доступ к всей информации без ограничений.
- c) Соблюдение этикета в цифровых коммуникациях.
- d) Предоставление всей информации сторонним организациям.

**6. Какие личные данные требуется защищать в профильной организации?**

- a) Имена и фамилии сотрудников.
- b) Информация о доходах сотрудников.
- c) Реквизиты документов сотрудников (паспорт, СНИЛС, ИНН).
- d) Все вышеперечисленное.

**7. Какую роль играет организационный уровень защиты информации?**

- a) Определяет политику безопасности и ответственность сотрудников за обработку информации.
- b) Защищает информацию с помощью аппаратных и программных средств.
- c) Обеспечивает физическую безопасность серверов и баз данных.
- d) Разрабатывает алгоритмы шифрования и аутентификации.

**8. Каковы основные принципы организационного уровня защиты информации?**

- a) Принцип наименьших привилегий, принцип обязательного доступа, принцип защиты в глубину.
- b) Принцип открытости, принцип свободного доступа, принцип минимизации затрат.
- c) Принцип безусловной доверенности, принцип неограниченной доступности, принцип саморегулирования.
- d) Принцип анонимности, принцип отсутствия контроля, принцип субъективности.

**9. Какие меры можно принять на процедурном уровне для защиты информации?**

- a) Регулярное обновление паролей, проведение аудита безопасности, обучение сотрудников правилам безопасного использования информации.
- b) Запрещение сотрудникам использовать цифровые технологии.
- c) Использование общедоступных сетей Wi-Fi для обмена конфиденциальной информацией.
- d) Предоставление доступа к информации без проверки подлинности.

**10. Какие меры можно предпринять для предотвращения утечки конфиденциальной информации?**

- a) Ограничение физического доступа к помещениям с конфиденциальной информацией, использование шифрования при передаче данных, установка системы мониторинга и обнаружения утечек.
- b) Открытый доступ к конфиденциальной информации для всех сотрудников.
- c) Сохранение конфиденциальной информации на обычных флеш-накопителях без шифрования.
- d) Проведение семинаров и тренингов по безопасности информации.

11. Какую роль играет обучение сотрудников в обеспечении информационной безопасности организации?

- a) Повышает осведомленность сотрудников о рисках и методах защиты информации.
- b) Отвечает за физическую безопасность организации.
- c) Укрепляет культуру безопасности и ответственность сотрудников.
- d) Разрабатывает технические меры защиты информации.

12. Какие меры можно принять для обеспечения безопасности электронной почты в организации?

- a) Использовать сильные пароли, шифровать сообщения, устанавливать антивирусное программное обеспечение.
- b) Публиковать конфиденциальные данные на публичных форумах.
- c) Использовать один и тот же пароль для всех аккаунтов.
- d) Отправлять конфиденциальные данные по электронной почте без шифрования.

13. Какие действия могут повредить репутацию организации в контексте информационной безопасности?

- a) Нарушение конфиденциальности персональных данных клиентов.
- b) Проведение аудита безопасности информационных систем.
- c) Регулярное обновление антивирусного программного обеспечения.
- d) Использование сильных паролей для всех учетных записей.

14. Каким образом можно улучшить информационную культуру в организации?

- a) Проводить регулярные тренинги и обучающие программы по безопасному использованию цифровых технологий.
- b) Запретить использование цифровых технологий в организации.
- c) Использовать старые и устаревшие программы и операционные системы.
- d) Предоставлять полный доступ к информации всем сотрудникам без ограничений.

15. Какие меры следует принять для защиты информации от внутренних угроз?

- a) Ограничить доступ к конфиденциальной информации только авторизованным сотрудникам.
- b) Не проверять подлинность идентификационных данных при доступе к информации.
- c) Установить программное обеспечение для мониторинга и обнаружения внутренних угроз.
- d) Предоставить всем сотрудникам полный доступ к конфиденциальной информации.

16. Что такое социальная инженерия и какие методы могут быть использованы злоумышленниками?

- a) Процесс манипулирования людьми с целью получения конфиденциальной информации; фишинг, поддельные звонки, поддельные письма.
- b) Защита информации от физических угроз; контроль доступа к зонам ограниченного доступа.
- c) Методы сканирования и обнаружения уязвимостей в сетевой инфраструктуре; тестирование на проникновение.
- d) Резервное копирование данных и восстановление после аварийных ситуаций.

17. Какие меры можно предпринять для защиты от взлома паролей?

- a) Использовать длинные и сложные пароли, использовать двухфакторную аутентификацию.
- b) Разглашать пароли своим коллегам для удобства работы.
- c) Использовать один и тот же пароль для всех аккаунтов.
- d) Оставлять записи с паролями на видном месте.

18. Что такое спам и какие меры можно принять для защиты от него?

- a) Нежелательная электронная почта; использование антиспам-фильтров, не разглашение личных данных в интернете.
- b) Использование вредоносных программ для получения конфиденциальной информации.
- c) Случайное получение электронных писем от незнакомых отправителей.
- d) Отправка электронных писем с конфиденциальной информацией без шифрования.

19. Какие признаки могут указывать на попытку социальной инженерии?

- a) Попытка получить конфиденциальную информацию по телефону или по электронной почте; требование срочного выполнения запроса.
- b) Использование сложных паролей для защиты информации.
- c) Открытое обсуждение конфиденциальных данных в общественных местах.
- d) Установка антивирусного программного обеспечения на компьютеры.

20. Как можно защитить себя от фишинга?

- a) Будьте осторожны при открытии электронных писем и ссылок от незнакомых отправителей.
- b) Проверяйте URL-адреса веб-сайтов перед вводом личных данных.
- c) Не раскрывайте личные данные, пароли или банковскую информацию в ответ на электронные запросы.
- d) Используйте защищенное соединение (HTTPS) при вводе конфиденциальной информации на веб-сайтах.

21. Какие меры можно предпринять для защиты от взлома аккаунтов на социальных сетях?

- a) Используйте уникальные и сложные пароли для каждого аккаунта.
- b) Активируйте двухфакторную аутентификацию для дополнительной защиты.
- c) Будьте осторожны с подозрительными ссылками и приложениями, которые запрашивают доступ к вашим аккаунтам.
- d) Регулярно проверяйте активность своих аккаунтов и изменяйте пароли, если есть подозрения в компрометации.

22. Какие организационные меры могут помочь в защите от утечки конфиденциальной информации?

- a) Ограничение доступа к конфиденциальной информации только необходимым сотрудникам.
- b) Обучение сотрудников правилам безопасности и конфиденциальности информации.
- c) Установка мощных физических барьеров для предотвращения несанкционированного доступа.
- d) Разглашение конфиденциальной информации в публичных источниках для привлечения внимания.

23. Какие меры можно предпринять для защиты своей конфиденциальности в цифровой среде?

- a) Будьте осторожны при размещении личной информации в социальных сетях и других публичных местах.
- b) Установите программное обеспечение для блокировки нежелательных отслеживаний и рекламы.
- c) Не делитесь личными данными с незнакомыми или непроверенными лицами и организациями.
- d) Регулярно проверяйте свои аккаунты на наличие несанкционированной активности и внешних вмешательств.

24. Как можно предотвратить утечку конфиденциальной информации при использовании общедоступных Wi-Fi сетей?

- a) Использовать виртуальную частную сеть (VPN) для шифрования интернет-соединения.
- b) Избегать передачи конфиденциальной информации, такой как пароли или банковские данные, через общедоступные Wi-Fi сети.
- c) Установить настройки безопасности на своем устройстве, чтобы избежать автоматического подключения к неизвестным сетям.
- d) Обновлять программное обеспечение и антивирусные программы на устройствах, чтобы предотвратить возможные уязвимости.

25. Какие меры безопасности можно принять при использовании электронной почты?

- a) Не открывать вложения или ссылки из непроверенных и подозрительных источников.
- b) Использовать сильные пароли для доступа к почтовым ящикам и регулярно менять их.
- c) Проверять адреса отправителей и подлинность писем, особенно при получении запросов на предоставление личной или финансовой информации.
- d) Внимательно ознакомиться с правилами использования электронной почты в организации и следовать им.

26. Какие меры безопасности можно принять для защиты от вирусов и вредоносных программ?

- a) Регулярно обновлять антивирусное программное обеспечение и выполнять сканирование компьютера на наличие угроз.
- b) Не открывать вложения или ссылки из ненадежных и незнакомых источников.
- c) Использовать брандмауэры и защищенные сетевые соединения для предотвращения несанкционированного доступа.
- d) Обучать сотрудников правилам безопасного поведения в интернете и распознаванию подозрительных ситуаций.

27. Какие меры безопасности следует принимать при использовании мобильных устройств?

- a) Установить пароль или использовать биометрическую аутентификацию для защиты доступа к устройству.
- b) Включить функцию удаленного управления и возможность удаленного стирания данных в случае утери или кражи устройства.
- c) Обновлять операционную систему и приложения на мобильном устройстве для исправления уязвимостей безопасности.
- d) Ограничить доступ к личным данным и приложениям на устройстве через настройки конфиденциальности.

28. Какие меры безопасности следует принимать при работе с конфиденциальной информацией на компьютере в общественном месте?

- a) Использовать защиту экрана (пароль или PIN-код) для блокировки компьютера при отсутствии пользователя.
- b) Избегать ввода конфиденциальной информации (пароли, банковские данные) в общественных местах.
- c) Убедиться, что Wi-Fi сеть, к которой подключен компьютер, безопасна и защищена.
- d) Закрывать все приложения и удалить временные файлы после завершения работы с конфиденциальной информацией.

29. Какие меры безопасности следует принимать при использовании съемных носителей данных (USB-флешки, внешние жесткие диски)?

- a) Проверять съемные носители на наличие вирусов перед их подключением к компьютеру.
- b) Не подключать съемные носители неизвестного происхождения или от ненадежных источников.
- c) Шифровать конфиденциальную информацию на съемных носителях для защиты от несанкционированного доступа.
- d) Регулярно резервировать данные с съемных носителей для предотвращения потери информации.

30. Какие меры безопасности следует принимать при использовании общих компьютеров в киберкафе или общественных местах?

- a) Не сохранять пароли, личные данные или другую конфиденциальную информацию на общих компьютерах.
- b) Закрывать все приложения и выходить из аккаунтов после окончания работы.
- c) Использовать режим инкогнито (приватный режим) при работе с конфиденциальной информацией.
- d) Избегать ввода банковских данных и иных конфиденциальных сведений.

**Критерии оценивания**

% верных ответов    Академическая оценка

0 – 60    Не зачтено

61 – 100    Зачтено

### 3. Контрольные вопросы и задания для проведения текущего контроля (примеры заданий практических работ)

Задание 1. Анализ информационной культуры организации: Исследуйте информационную культуру конкретной организации и определите ее уровень развития. Проведите опрос или интервьюирование сотрудников, анализируйте доступные документы и ресурсы организации. Подготовьте отчет, в котором вы оцениваете сильные и слабые стороны информационной культуры и предлагаете рекомендации по ее улучшению.

Задание 2. Создание политики информационной безопасности: Разработайте политику информационной безопасности для организации. Определите основные принципы, правила и процедуры, которые должны соблюдаться сотрудниками для обеспечения безопасного использования цифровых технологий и защиты конфиденциальной информации. Подготовьте документ, который описывает политику информационной безопасности и предлагает меры по ее внедрению и контролю.

Задание 3. Обучение сотрудников по легальному использованию цифровых технологий: Разработайте образовательную программу или тренинг, который поможет сотрудникам организации разобраться с основными аспектами легального использования цифровых технологий. Включите в программу информацию о правовых аспектах авторских прав, лицензирования программного обеспечения и защиты данных. Проведите обучение и оцените его результаты.

Задание 4. Аудит цифровой среды организации: Проведите аудит цифровой среды в организации, чтобы оценить ее готовность к использованию современных технологий и ресурсов. Оцените наличие необходимых инфраструктурных элементов, таких как компьютеры, программное обеспечение, сетевое оборудование. Также проанализируйте политики и процедуры, связанные с использованием цифровых технологий. Подготовьте отчет, в котором вы описываете результаты аудита и рекомендации по улучшению цифровой среды.

Задание 5. Разработка программы информационной грамотности: Создайте программу по развитию информационной грамотности среди сотрудников организации. Определите ключевые компетенции, которые необходимо развить, такие как критическое мышление, оценка и выбор качественной информации, эффективное использование поисковых систем и баз данных. Разработайте учебные материалы, задания и тесты, которые помогут сотрудникам развить эти навыки. Проведите обучение с использованием разработанной программы и оцените его результаты.

Задание 6. Анализ правовых аспектов цифровой среды: Исследуйте правовые аспекты, связанные с цифровой средой в конкретной организации или отрасли. Изучите законы и нормативные акты, регулирующие использование цифровых технологий и обработку данных. Определите существующие риски и проблемы в области законности и безопасности использования цифровых технологий. Подготовьте отчет, в котором вы анализируете правовую ситуацию и предлагаете рекомендации по улучшению соблюдения законодательства.

Задание 7. Разработка стратегии цифровой трансформации организации: Разработайте стратегию цифровой трансформации для организации, которая включает в себя планы по внедрению новых цифровых технологий, обучению сотрудников и развитию информационной культуры. Определите цели, этапы внедрения и меры по оценке результатов. Подготовьте презентацию, в которой представите разработанную стратегию и обоснуйте ее важность и выгоды для организации.

Задание 8. Анализ уязвимостей информационной безопасности: Проведите анализ уязвимостей информационной безопасности в организации. Исследуйте возможные угрозы, связанные с взломом, несанкционированным доступом и утечкой данных. Оцените существующие меры безопасности и определите их эффективность. Разработайте рекомендации по устранению выявленных уязвимостей и повышению уровня информационной безопасности.

Задание 9. Разработка политики цифровой этики: Создайте политику цифровой этики для организации, которая определит правила и нормы поведения в цифровой среде. Включите в политику вопросы конфиденциальности,уважительного общения в онлайн-среде, этики использования цифровых ресурсов и защиты личных данных. Определите ответственности сотрудников и ожидания организации относительно их поведения в цифровой среде. Разработайте документ, который описывает политику цифровой этики и предлагает меры по ее внедрению и соблюдению.

Задание 10. Планирование и проведение семинара по информационной культуре: Организуйте семинар по тематике информационной культуры, цифровой среды и безопасного использования цифровых технологий. Подготовьте программу мероприятия, включающую доклады, панельные дискуссии и практические мастер-классы. Укажите потенциальных экспертов и специалистов в области информационной культуры для выступлений. Оцените эффективность семинара на основе обратной связи участников и результатов обучающих мероприятий.

Задание 11. Напишите краткое руководство по созданию надежных паролей, включающее рекомендации по длине, сложности и регулярной смене паролей.

Разработайте план обеспечения физической безопасности офиса или компьютерной лаборатории, включающий меры по контролю доступа, видеонаблюдению и защите оборудования.

Задание 12. Составьте список политик безопасности информации, которые должны быть реализованы в организации, и опишите процедуры и меры, необходимые для их соблюдения. Проведите анализ уязвимостей сети организации и предложите рекомендации по устранению выявленных уязвимостей и улучшению общей безопасности. Создайте обучающий материал или презентацию, объясняющую основные принципы социальной инженерии и методы защиты от таких атак.

**Критерии оценивания**

Характеристика ответа

Академическая оценка

Демонстрируемое практическое решение недостаточно или полностью не соответствует условиям задания

Не зачтено

Демонстрируемое практическое решение в большей мере или полностью

соответствует условиям задания

Зачтено

**5.2. Темы письменных работ**

1. Роль информационной культуры в современной организации.
2. Влияние цифровой среды на развитие организации.
3. Преимущества и риски использования цифровых технологий в организационной среде.
4. Основные принципы информационной безопасности в организации.
5. Цифровая этика и ее значение для организаций.
6. Внедрение цифровых технологий в управленческие процессы организации.
7. Легальные аспекты использования цифровых технологий в организации.
8. Кибербезопасность и защита информации в организационной среде.
9. Роль лидерства в формировании информационной культуры организации.
10. Информационное самоопределение сотрудников в цифровой среде.
11. Использование социальных медиа в организационных коммуникациях.
12. Преимущества цифровых инструментов в организации проектной работы.
13. Цифровое образование и его влияние на профессиональное развитие сотрудников.
14. Использование больших данных для принятия управленческих решений в организации.
15. Роль цифровой трансформации в развитии организаций.
16. Инновационные методы обучения и тренинга в цифровой среде.
17. Создание безопасной цифровой рабочей среды для сотрудников организации.
18. Влияние цифровой среды на развитие командной работы в организации.
19. Роль правовых аспектов в использовании цифровых технологий в организации.
20. Эффективное управление информацией и знаниями в цифровой среде организации.

**Критерии оценивания**

Характеристика ответа

Академическая оценка

В ответе не содержится подробного и понятного ответа на вопрос, раскрывающего содержание темы работы, искажены факты, присутствуют недостоверные сведения, устаревшие данные

Не зачтено

В ответе содержится подробный и понятный ответ на вопрос, раскрывающий содержание темы работы, не искажены факты, отсутствуют недостоверные сведения, устаревшие данные

Зачтено

**5.3. Фонд оценочных средств****1. Вопросы и задания для проведения устного собеседования на зачете**

1. Что такое информационная культура и какие составляющие в нее входят?
2. Какие основные принципы лежат в основе цифровой среды?
3. Какие основные компоненты включает в себя цифровая среда в организации?
4. Какие преимущества предоставляет цифровая среда для организации?
5. Какие основные принципы легального использования цифровых технологий нужно соблюдать?
6. Какие меры безопасности необходимо принять при использовании цифровых технологий в организации?
7. Какие правовые аспекты необходимо учитывать при сборе и хранении личных данных?
8. Что такое кибербезопасность и какие методы можно применить для защиты информации организации?
9. Как можно развивать информационную культуру среди сотрудников организации?
10. Какие негативные последствия могут возникнуть при неправильном использовании цифровых технологий?
11. Какие основные принципы этического поведения в цифровой среде нужно соблюдать?
12. Какие технологические тренды в области цифровых технологий могут повлиять на организацию?
13. Какие инструменты и ресурсы могут быть использованы для повышения информационной грамотности сотрудников организации?
14. Как организация может эффективно использовать социальные сети в своей деятельности?
15. Какие меры можно принять для защиты интеллектуальной собственности в цифровой среде?
16. Какие меры можно принять для предотвращения кибератак и внешних угроз в организации?
17. Что такое «цифровой след» и как он может повлиять на частную жизнь сотрудников организации?
18. Какие навыки и компетенции в области цифровых технологий являются важными для современных профессионалов?
19. Какие принципы эффективного управления информацией и знаниями применимы в организации?
20. Как можно улучшить информационную безопасность в организации?
21. Какие меры необходимо предпринять для защиты конфиденциальности данных клиентов в цифровой среде?
22. Какие правила и нормы этики следует соблюдать при использовании электронной почты и других коммуникационных средств в организации?
23. Какие методы аутентификации и авторизации могут быть использованы для обеспечения безопасности доступа к информационным системам организаций?
24. Какие риски связаны с использованием облачных сервисов, и как можно снизить эти риски?

25. Какие основные принципы разработки безопасных и надежных веб-сайтов и приложений следует учитывать?
26. Какие основные законы и нормативные акты регулируют использование цифровых технологий в организациях?
27. Как можно организовать эффективную систему резервного копирования данных для предотвращения их потери или повреждения?
28. Какие основные принципы информационной безопасности следует учитывать при использовании мобильных устройств в организации?
29. Какие требования к обработке персональных данных установлены законодательством, и как они влияют на деятельность организаций?
30. Какие основные принципы информационной грамотности должны учитываться при работе с цифровыми технологиями?
31. Какие меры предпринимаются для защиты интеллектуальной собственности в цифровой среде?
32. Какие методы шифрования данных используются для обеспечения их конфиденциальности и целостности?
33. Какие основные угрозы информационной безопасности могут возникать при использовании социальных сетей, и как их предотвращать?
34. Как можно обеспечить безопасность и надежность проведения электронных платежей и транзакций в цифровой среде?
35. Что такое цифровой этикет и почему он важен в современном общении?
36. Какие основные принципы цифрового этикета следует соблюдать при отправке электронных писем?
37. Какие правила поведения следует придерживаться в социальных сетях с точки зрения цифрового этикета?
38. Каким образом можно поддерживать положительный и уважительный тон в онлайн-дискуссиях и комментариях?
39. Какие меры безопасности и конфиденциальности необходимо соблюдать при использовании цифровых коммуникаций и социальных медиа?

#### Критерии оценивания

Характеристика ответа	Академическая оценка	
В ответе не содержатся подробные и понятные сведения по содержанию в задании	Не засчитано	
В ответе присутствует достаточное количество подробных и понятных сведений по содержанию в задании		Засчитано

#### 2. Практическое задание для выполнения на зачете

Продемонстрировать и пояснить решение одного из заданий практических работ. Объяснить особенности использованных инструментов.

#### Критерии оценивания

«Не засчитано» выставляется, если демонстрируемое практическое решение недостаточно или полностью не соответствует условиям задания или обучающийся полностью затрудняется его представить, либо не является авторским.

«Засчитано» выставляется, если демонстрируемое практическое решение в большей мере или полностью соответствует условиям задания, ясно объясняется и выполнено лично автором.

#### 5.4. Перечень видов оценочных средств

<b>6. УЧЕБНО-МЕТОДИЧЕСКОЕ И ИНФОРМАЦИОННОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ (МОДУЛЯ)</b>			
<b>6.1. Рекомендуемая литература</b>			
<b>6.1.1. Основная литература</b>			
	Авторы, составители	Заглавие	Издательство, год
Л1.1	Скоробогатов А. В., Борисова Н. Р.	Нормативно-правовое обеспечение образования: учебное пособие	Казань: Познание (Институт ЭУП), 2014
Л1.2	Николюкин С. В.	Правовое обеспечение профессиональной деятельности: учебник и практикум для СПО	Москва: Юрайт, 2022
Л1.3	Афанасьев И. В., Афанасьева И. В.	Правовые основы профессиональной деятельности: учебное пособие для вузов	Москва: Юрайт, 2022
Л1.4	Хисматов Р. Г., Сафин Р. Г., Тунцев Д. В., Тимербаев Н. Ф.	Современные компьютерные технологии: учебное пособие	Казань: Казанский научно-исследовательский технологический университет (КНИТУ), 2014
Л1.5	Прохорова О. В.	Информационная безопасность и защита информации: учебник	Самара: Самарский государственный архитектурно-строительный университет, 2014

	Авторы, составители	Заглавие	Издательство, год
Л1.6	Громов Ю. Ю., Дидрих И. В., Иванова О. Г., и др.	Информационные технологии: учебник	Тамбов: Тамбовский государственный технический университет (ТГТУ), 2015
Л1.7	Ищенинов В. Я.	Информационная безопасность и защита информации: теория и практика: учебное пособие	Москва, Берлин: Директ-Медиа, 2020
Л1.8	Граецкая О. В., Чусова Ю. С.	Информационные технологии поддержки принятия решений: учебное пособие	Ростов-на-Дону, Таганрог: Южный федеральный университет, 2019
Л1.9	Гаврилов М. В., Климов В. А.	Информатика и информационные технологии: учебник для вузов	Москва: Юрайт, 2022
Л1.10	Гендина Н. И., Косолапова Е. В., Рябцева Л. Н.	Информационная культура личности в 2 ч. Часть 2: учебное пособие для вузов	Москва: Юрайт, 2022
Л1.11	Гендина Н. И., Косолапова Е. В., Рябцева Л. Н.	Информационная культура личности в 2 ч. Часть 1: учебное пособие для вузов	Москва: Юрайт, 2022
Л1.12	Рязанова З. Г.	Информационная культура и технологии в образовании: лабораторный практикум: лабораторный практикум	Красноярск: КГПУ им. В. П. Астафьева, 2018

#### 6.1.2. Дополнительная литература

	Авторы, составители	Заглавие	Издательство, год
Л2.1	Соловова Н. В., Суханкина Н. В., Дмитриева Д. С., Дмитриев Д. С.	Цифровая педагогика: технологии и методы: учебное пособие	Самара: Самарский национальный исследовательский университет имени академика С.П. Королева (Самарский университет), 2020
Л2.2	Рыбцова Л. Л., Дудина М. Н., Гречухина Т. И., Вершинина Т. С., Усачева А. В., Вороткова И. Ю.	Современные образовательные технологии: учебное пособие для вузов	Москва: Юрайт, 2022

#### 6.1.3. Методические разработки

	Авторы, составители	Заглавие	Издательство, год
Л3.1	Смирнова Л. О., Мозговой М. В., Дзюина И. В., Чувакова В. Г., Мельситова В. А., Савицкий К. Л., Валькова Ю. Е., Дудко В. В.	Использование деятельностного подхода в проектах цифровой трансформации в образовании: учебное пособие для вузов	Москва: Юрайт, 2022
Л3.2	Дорошенко В. Ю., Зотова Л. И., Лавриненко В. Н., Островский Э. В., Подвойская Л. Т.	Психология и этика делового общения: учебник	Москва: Юнити-Дана, 2015

#### 6.3.1 Лицензионное и свободно распространяемое программное обеспечение, в том числе отечественного производства

Для освоения дисциплины необходим компьютер с графической операционной системой, офисным пакетом приложений, интернет-браузером, программой для чтения PDF-файлов, программой для просмотра изображений и видеофайлов и программой для работы с архивами.

### 6.3.2 Перечень профессиональных баз данных и информационных справочных систем

1. Elibrary.ru: электронная библиотечная система : база данных содержит сведения об отечественных книгах и периодических изданиях по науке, технологии, медицине и образованию. Адрес: <http://elibrary.ru>. Режим доступа: Индивидуальный неограниченный доступ.
2. Электронно-библиотечная система «Университетская библиотека онлайн». Адрес: <https://biblioclub.ru>. Режим доступа: Индивидуальный неограниченный доступ.
3. Электронно-библиотечная система издательства «ЛАНЬ». Адрес: [e.lanbook.com](http://e.lanbook.com). Режим доступа: Индивидуальный неограниченный доступ.
4. Образовательная платформа «Юрайт». Адрес: <https://urait.ru>. Режим доступа: Индивидуальный неограниченный доступ.
5. ИС Антиплагиат: система обнаружения заимствований. Адрес: <https://krasspu.antiplagiat.ru>. Режим доступа: Индивидуальный неограниченный доступ.

### 7. МТО (оборудование и технические средства обучения)

Перечень учебных аудиторий и помещений закрепляется ежегодным приказом «О закреплении аудиторий и помещений в

### 8. МЕТОДИЧЕСКИЕ УКАЗАНИЯ ДЛЯ ОБУЧАЮЩИХСЯ ПО ОСВОЕНИЮ ДИСЦИПЛИНЫ (МОДУЛЯ)

Основными видами аудиторной работы по дисциплине «Информационная культура профильной организации» для обучающихся являются лекционные и практические занятия. В ходе лекций преподаватель излагает и разъясняет основные, наиболее сложные понятия темы, а также связанные с ней теоретические и практические проблемы, дает рекомендации на практические занятия, вместе с тем, четко формулирует и указания на самостоятельную работу.

В ходе лекционных занятий необходимо вести конспектирование учебного материала. Обращать внимание на категории, формулировки, раскрывающие содержание тех или иных явлений и процессов, научные выводы и практические рекомендации, положительный опыт в изучении проблем. Знакомство с дисциплиной происходит уже на первой лекции, где от студента требуется не просто внимание, но и самостоятельное оформление конспекта.

При работе с конспектом лекций необходимо учитывать тот фактор, что одни лекции дают ответы на конкретные вопросы темы, другие – лишь выявляют взаимосвязи между явлениями, помогая студенту понять глубинные процессы развития изучаемого предмета как в историческом аспекте, так и в настоящее время. Конспектирование лекций – сложный вид вузовской аудиторной работы, предполагающий интенсивную умственную деятельность студента. Конспект является полезным тогда, когда записано самое существенное и сделано это самим обучающимся.

Целесообразно разработать собственную систему сокращений, аббревиатур и символов. Однако при дальнейшей работе с конспектом символы лучше заменить обычными словами для быстрого зрительного восприятия текста. 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 теоретическими знаниями.

Практические занятия позволяют интегрировать теоретические знания и формировать практические умения и навыки студентов в процессе учебной деятельности. Структура и последовательность занятий: на первом, вводном, занятии проводится инструктаж обучающихся по охране труда, технике безопасности и правилам работы в лаборатории по

инструкциям утвержденного образца с фиксацией результатов в журнале инструктажа. Обучающиеся также знакомятся с основными требованиями преподавателя по выполнению учебного плана, с графиком прохождения лабораторных занятий, с графиком прохождения контрольных заданий, с основными формами отчетности по выполненным работам и заданиям. При изучении лекционного материала вам необходимо будет использовать как выложенные в электронном курсе опорные презентации и сопроводительные материалы, так и дополнительные статьи из периодических изданий и зарубежных источников. Освоение данной дисциплины требует также активного использования возможностей Интернет-ресурсов, что позволяет значительно обогатить используемый в практике материал, а также способствует развитию вашей профессиональной компетентности в области использования возможностей информационных систем в будущей деятельности.

В ходе занятий необходимо быть готовыми использовать новые информационные технологии, в частности, использовать средства мультимедийных аудиторий. Лекционный материал будет сопровождаться использованием в ходе занятий средств повышения наглядности представляемых материалов (наглядных пособий, аудиовизуальных средств обучения, интерактивных заданий и упражнений), чтобы сформировать у вас понимание, умения и навыки их применения в практической деятельности.

Особое внимание необходимо уделять изучению понятийного аппарата дисциплины. Лекции ориентированы на систематизированное представление знаний, раскрытие сущности наиболее трудных для освоения учебных вопросов (материалов). При посещении лекции нужно учитывать, что затем будет проводиться практическое, следует делать краткие записи в виде конспекта, задавать преподавателю вопросы относительно дальнейшего применения лекционного материала на практических занятиях и промежуточной аттестации (контрольной работе, тестировании, зачете, экзамене) по каждой теме.

Лабораторные занятия могут включать такие виды деятельности, как организация группового обсуждения студентами проблем по предлагаемым темам в рамках определенного раздела изучаемой дисциплины; анализа, проведения, обработки и интерпретации результатов изучения различных информационных источников; изучения характеристик и возможностей средств различных научных отраслей; практической отработки навыков применения теоретических знаний на практике; обсуждения выполненных в ходе занятия работ (заданий).

В качестве текущего контроля успеваемости на занятиях используются комплексные профессионально-ориентированные задания (кейсы), которые в данном курсе могут быть обязательными и дополнительными. Практические задания потребуют от вас решения конкретных задач и проблем, моделирования поведения в ситуациях, принятия решений и активных действий согласно собственному плану. При текущем контроле преподаватель будет в первую очередь обращать внимание на проявление у вас признаков информационной культуры, сформированность исследовательских навыков, способность аргументировать свою позицию, развитие навыков обоснования выполненных действий, способность действовать

самостоятельно.

Преподаватель в течение всего семестра будет оценивать вашу активность и качество выполнения всех заданий, при этом активно помогая тем, кто испытывает определенные затруднения при изучении материалов учебной дисциплины, при помощи консультаций, дополнительных пояснений или специальных дополнительных материалов и заданий.

Итоговой формой контроля работы по дисциплине является зачет.

Критериями для допуска к прохождению промежуточной аттестации являются:

- а) успешное выполнение и сдача всех обязательных заданий в текущем семестре;
- б) наличие посещаемости большей части (60% и более) очных занятий и/или активности в электронном курсе (изучение не менее 70% ресурсов).

К зачету необходимо будет подготовиться, опираясь на список заданий и вопросов для устного собеседования. В качестве источников для ответов на зачетные задания можно использовать рекомендованные данной программой учебники и учебные пособия, материалы занятий, ресурсы электронного курса, а также самостоятельно обнаруженные цифровые ресурсы образовательного характера.