

Министерство культуры Российской Федерации
ФГБОУ ВО «Кемеровский государственный институт культуры»
Факультет информационных, библиотечных и музейных технологий
Кафедра цифровых технологий и ресурсов

ФОНД ОЦЕНОЧНЫХ СРЕДСТВ

по учебной дисциплине

ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ И ЗАЩИТА ИНФОРМАЦИИ

Направление подготовки

42.03.05 «Медиакоммуникации»

Профили подготовки

Медиакоммуникации в коммерческой и социальной сферах

Квалификация (степень) выпускника
бакалавр

Форма обучения
Очная, заочная

Утвержден на заседании
кафедры
ЦТиР, 23.05.2022 г., протокол
№ 10.

Составитель
Мишова В.В.

Кемерово

Фонд оценочных средств

1. Перечень оцениваемых компетенций:

- УК-2. Способен определять круг задач в рамках поставленной цели и выбирать оптимальные способы их решения, исходя из действующих правовых норм, имеющихся ресурсов и ограничений

2. Критерии и показатели оценивания компетенций

Обучающийся должен демонстрировать следующие результаты обучения по дисциплине:

знать:

- компоненты концептуальной модели информационной безопасности (31);
- задачи и функции защиты электронных информационных ресурсов (32);
- характеристики информационных систем, влияющие на безопасность информации (33);
- классификацию и характеристику угроз информационной безопасности (34);
- классификацию преступлений в сфере информационной безопасности (35);
- нормативно-правовые документы в области защиты информации (36);
- состав организационных документов обеспечения информационной безопасности (37);
- классификацию средств программно-технической защиты информации (38);
- требования к комплексной системе защиты информации в организации (39);

уметь:

- выявлять угрозы информационной безопасности (У1);
- применять на практике нормативно-правовые документы в области защиты информации (У2);
- принимать решения в организации информационной безопасности (У3);
- обосновывать и осуществлять выбор средств защиты информации (У4);
- использовать современные методы и средства в комплексной системе защиты информации (У5);

владеть:

- терминологией в сфере информационной безопасности (В1);
- способами предотвращения случайных и преднамеренных угроз информационной безопасности (В2);
- готовностью к разработке политики информационной безопасности (В3);
- навыками работы с программно-техническими средствами обеспечения информационной безопасности, используемых в организации (В4);
- способностью формулировать требования к системе защиты информации (В5).

3. Формируемые компетенции в структуре учебной дисциплины и средства их оценивания

№ п/п	Разделы (темы) дисциплины	Код оцениваемой компетенции	Планируемые результаты обучения по дисциплине (ЗУВ)	Оценочное средство
1	Раздел 1. Информационная безопасность: общая характеристика			
1.1	Информационная безопасность: определение понятия, состав, назначение	УК-2	31, В1	проверка результатов выполнения практической работы
1.2	Информационная система как объект	УК-2	32, 33, В1	проверка результатов выполнения

	защиты			практической работы
1.3	Угрозы информационной безопасности в информационных системах	УК-2	34, 35, У1, В2, В1	проверка результатов выполнения практической работы
2	Раздел 2. Обеспечение информационной безопасности организации			
2.1	Правовое обеспечение информационной безопасности организации	УК-2	36, У2, В1	проверка результатов выполнения практической работы
2.2	Организационное обеспечение информационной безопасности организации	УК-2	37, У3, В3	проверка результатов выполнения практической работы
2.3	Программно-техническое обеспечение информационной безопасности организации	УК-2	38, У4, В4	проверка результатов выполнения практической работы, тестирование
2.4	Комплексная система защиты информации в организации	УК-2	39, У5, В5	реализация учебного проекта

4. Оценочные средства по дисциплине для текущего контроля

4.1. Описание критериев оценивания компетенций на различных уровнях их формирования

При выставлении оценки преподаватель учитывает: логику, структуру, стиль ответа; культуру речи, манеру общения; готовность к дискуссии, аргументированность ответа; уровень самостоятельного мышления; умение приложить теорию к практике, решить задачи.

Нулевой уровень («неудовлетворительно»). Результаты обучения студента свидетельствуют:

З) об усвоении им некоторых элементарных знаний, но студент не владеет понятийным аппаратом изучаемой предметной области (учебной дисциплины);

У) не умеет установить связь теории с практикой;

В) не владеет способами решения практико-ориентированных задач.

Первый уровень - пороговый («удовлетворительно»). Достигнутый уровень оценки результатов обучения студента показывает:

З) знания имеют фрагментарный характер, отличаются поверхностностью и малой содержательностью; студент раскрывает содержание вопроса, но не глубоко, бессистемно, с некоторыми неточностями;

У) слабо, недостаточно аргументированно может обосновать связь теории с практикой;

В) способен понимать и интерпретировать основной теоретический материал по дисциплине.

Второй уровень повышенный («хорошо»). Студент на должном уровне:

З) раскрывает учебный материал: даёт содержательно полный ответ, требующий незначительных дополнений и уточнений, которые он может сделать самостоятельно после наводящих вопросов преподавателя;

У) демонстрирует учебные умения и навыки в области решения практико-ориентированных задач;

В) владеет способами анализа, сравнения, обобщения и обоснования выбора методов решения практико-ориентированных задач.

Третий уровень продвинутый («отлично»). Студент, достигающий должного уровня:

З) даёт полный, глубокий, выстроенный логично по содержанию вопроса ответ, используя различные источники информации, не требующий дополнений и уточнений;

У) доказательно иллюстрирует основные теоретические положения практическими примерами;

В) способен глубоко анализировать теоретический и практический материал, обобщать его, самостоятельно делать выводы, вести диалог и высказывать свою точку зрения.

4.2. Критерии оценивания практических работ

В ходе освоения учебной дисциплины предусмотрено 12 практических работ. Описания практических работ представлены в электронном учебно-методическом комплексе дисциплины, размещенном на сайте «Электронная образовательная среда КемГИК»).

Критерии оценивания:

- выполнены все задания в практической работе, студент обнаруживает полное понимание материала, соблюдает требования к представлению результатов выполнения заданий практической работы - **5 баллов**;
- выполнены все задания в практической работе, студент соблюдает требования к представлению результатов выполнения заданий практической работы, однако допускает единичные ошибки, неточности - **4 балла**;
- выполнена большая часть заданий в практической работе, студент знает и понимает основные положения данной темы, но допускает единичные ошибки; студент в целом соблюдает требования к представлению результатов выполнения заданий практической работы, но допускает единичные неточности- **3 балла**;
- выполнено меньше половины заданий практической работы, некоторые задания выполнены не в полном объеме или допущены единичные ошибки, неточности, студент нарушает некоторые требования к представлению результатов выполнения заданий практической работы - **2 балла**;
- выполнено меньше половины заданий практической работы, задания выполнены не в полном объеме или допущены ошибки, неточности, студент нарушает требования к представлению результатов выполнения заданий практической работы- **1 балл**;
- практическая работа не выполнена - **0 баллов**.

Максимальное количество баллов – 60.

4.3. Критерии оценивания учебных исследовательских проектов

Тема проекта выбирается из списка, рекомендованного преподавателем; также возможен вариант самостоятельного выбора студентом темы, при условии обязательного согласования с преподавателем.

Защита проекта – публичное выступление, представляющее собой развернутое изложение исследованной проблемы. Продолжительность выступления – до 10 мин.

Выполняемые студентами проекты оцениваются по каждому из представленных критериев:

Тема проекта выбирается из списка, рекомендованного преподавателем; также возможен вариант самостоятельного выбора студентом темы, при условии обязательного согласования с преподавателем.

Выполняемые студентами проекты оцениваются по каждому из представленных критериев:

Наименование критерия	Максимальное количество баллов
<i>Критерии оценки проекта</i>	

Соответствие содержания проекта заданной теме	2
Обоснованность результатов представленной работы	2
Грамотное использование цветового и шрифтового оформления	2
Качество представления графического материала, звуковой и видеоинформации	2
Гармоничность сочетания различных форм представления информации	2
Четкость и логичность выводов	2
Качество оформления отчета о выполненном проекте и презентации (отсутствие орфографических и синтаксических ошибок)	2
<i>Критерии оценки выступлений</i>	
Грамотность и логичность изложения материала	2
Глубина владения материалом	2
Аргументированность ответов на вопросы	2
	20

Каждый из критериев оценивается от 0 до 2 баллов, 1 – критерий выполнен частично, 2 – критерий выполнен в полном объеме. Таким образом, максимальное количество баллов за выполнение и защиту проекта составляет **20 баллов**.

5. Оценочные средства по дисциплине для промежуточного контроля

5.1. Вопросы к зачету

Обязательным условием получения зачета является выполнение всех практических заданий по курсу, защита реферата и прохождение тестовых заданий. Среднее арифметическое значение всех полученных оценок в ходе текущей аттестации может служить основанием для получения зачета.

В тестовом задании представлены вопросы, которые имеют закрытый и открытый характер.

Вопрос	Ответ
1. ВЫБРАТЬ ВАРИАНТЫ ПРАВИЛЬНОГО ОТВЕТА <i>Какие существуют основные уровни обеспечения защиты информации?</i> <ul style="list-style-type: none"> а) Законодательный б) Организационно-административный в) Программно-технический (аппаратный) г) Физический д) Вероятностный е) Распределительный 	<ul style="list-style-type: none"> а) Законодательный б) Организационно-административный в) Программно-технический (аппаратный) г) Физический
2. ВЫБРАТЬ ВАРИАНТЫ ПРАВИЛЬНОГО ОТВЕТА <i>Какие основные свойства информации и систем обработки информации необходимо поддерживать, обеспечивая информационную безопасность?</i> <ul style="list-style-type: none"> а) Доступность б) Целостность в) Конфиденциальность г) Управляемость д) Сложность 	<ul style="list-style-type: none"> а) Доступность б) Целостность в) Конфиденциальность
3. ВЫБРАТЬ ВАРИАНТЫ ПРАВИЛЬНОГО ОТВЕТА <i>Что такое доступность информации?</i> <ul style="list-style-type: none"> а) Свойство системы, в которой циркулирует информация, характеризующееся способностью обеспечивать своевременный беспрепятственный 	<ul style="list-style-type: none"> а) Свойство системы, в которой циркулирует информация, характеризующееся способностью

<p>доступ к информации субъектов, имеющих на это надлежащие полномочия</p> <p>б) Свойство системы, обеспечивать беспрепятственный доступ к информации любых субъектов</p> <p>в) Свойство системы, обеспечивать закрытый доступ к информации любых субъектов</p> <p>г) Свойство информации, заключающееся в легкости ее несанкционированного получения и дальнейшего распространения (несанкционированного копирования)</p>	<p>обеспечивать своевременный беспрепятственный доступ к информации субъектов, имеющих на это надлежащие полномочия</p>
<p>4. ВЫБРАТЬ ВАРИАНТ ПРАВИЛЬНОГО ОТВЕТА</p> <p><i>Что такое целостность информации?</i></p> <p>а) Свойство информации, заключающееся в ее существовании в неискаженном виде (неизменном по отношению к некоторому фиксированному ее состоянию)</p> <p>б) Свойство информации, заключающееся в возможности ее изменения любым субъектом</p> <p>в) Свойство информации, заключающееся в возможности изменения только единственным пользователем</p> <p>г) Свойство информации, заключающееся в ее существовании в виде единого набора файлов</p>	<p>а) Свойство информации, заключающееся в ее существовании в неискаженном виде (неизменном по отношению к некоторому фиксированному ее состоянию)</p>
<p>5. ВЫБРАТЬ ВАРИАНТ ПРАВИЛЬНОГО ОТВЕТА</p> <p><i>Что такое конфиденциальность информации?</i></p> <p>а) Свойство информации, указывающее на необходимость введения ограничений на круг субъектов, имеющих доступ к данной информации, и обеспечиваемое способностью системы сохранять указанную информацию в тайне от субъектов, не имеющих полномочий на право доступа к ней</p> <p>б) Свойство информации, заключающееся в ее существовании в неискаженном виде (неизменном по отношению к некоторому фиксированному ее состоянию)</p> <p>в) Свойство информации, заключающееся в ее существовании в виде не защищенного паролем набора</p> <p>г) Свойство информации, заключающееся в ее шифровании</p> <p>д) Свойство информации, заключающееся в ее принадлежности к определенному набору</p>	<p>а) Свойство информации, указывающее на необходимость введения ограничений на круг субъектов, имеющих доступ к данной информации, и обеспечиваемое способностью системы сохранять указанную информацию в тайне от субъектов, не имеющих полномочий на право доступа к ней</p>
<p>6. ВЫБРАТЬ ВАРИАНТЫ ПРАВИЛЬНОГО ОТВЕТА</p> <p><i>Что относится к угрозам информационной безопасности?</i></p> <p>а) Потенциально возможное событие, действие, процесс или явление, которое может привести к нарушению конфиденциальности, целостности, доступности информации, а также неправомерному ее тиражированию</p> <p>б) Классификация информации</p> <p>в) Стихийные бедствия и аварии (наводнение, ураган, землетрясение, пожар и т.п.)</p>	<p>а) Потенциально возможное событие, действие, процесс или явление, которое может привести к нарушению конфиденциальности, целостности, доступности информации, а также неправомерному ее тиражированию</p> <p>в) Стихийные бедствия и аварии (наводнение, ураган,</p>

<p>г) Сбои и отказы оборудования (технических средств) АС</p> <p>д) Ошибки эксплуатации (пользователей, операторов и другого персонала)</p> <p>е) Преднамеренные действия нарушителей и злоумышленников (обиженных лиц из числа персонала, преступников, шпионов, диверсантов)</p> <p>ж) Последствия ошибок проектирования и разработки компонентов АС (аппаратных средств, технологии обработки информации, программ, структур данных и т.п.)</p> <p>з) Иерархическое расположение данных</p>	<p>землетрясение, пожар и т.п.)</p> <p>г) Сбои и отказы оборудования (технических средств) АС</p> <p>д) Ошибки эксплуатации (пользователей, операторов и другого персонала)</p> <p>е) Преднамеренные действия нарушителей и злоумышленников (обиженных лиц из числа персонала, преступников, шпионов, диверсантов)</p> <p>ж) Последствия ошибок проектирования и разработки компонентов АС (аппаратных средств, технологии обработки информации, программ, структур данных и т.п.)</p>
<p>7. ВЫБРАТЬ ВАРИАНТ ПРАВИЛЬНОГО ОТВЕТА</p> <p><i>Какое определение информации дано в Законе РФ "Об информации, информатизации и защите информации"?</i></p> <p>а) Сведения о лицах, предметах, фактах, событиях, явлениях и процессах, независимо от формы их представления</p> <p>б) Получение сведений из глобальной информационной сети</p> <p>в) Систематизированные данные об экономике</p> <p>г) Это результаты компьютерных решений определенных задач</p>	<p>а) Сведения о лицах, предметах, фактах, событиях, явлениях и процессах, независимо от формы их представления</p>
<p>8. ВЫБРАТЬ ВАРИАНТ ПРАВИЛЬНОГО ОТВЕТА</p> <p><i>Что относится к правовым мерам защиты информации?</i></p> <p>а) Законы, указы и другие нормативные акты, регламентирующие правила обращения с информацией и ответственность за их нарушения</p> <p>б) Действия правоохранительных органов для защиты информационных ресурсов</p> <p>в) Организационно-административные меры для защиты информационных ресурсов</p> <p>г) Действия администраторов сети защиты информационных ресурсов</p>	<p>а) Законы, указы и другие нормативные акты, регламентирующие правила обращения с информацией и ответственность за их нарушения</p>
<p>9. ВЫБРАТЬ ВАРИАНТЫ ПРАВИЛЬНОГО ОТВЕТА</p> <p><i>Какие правовые документы решают вопросы информационной безопасности?</i></p> <p>а) Уголовный кодекс РФ</p> <p>б) Конституция РФ</p> <p>в) Закон "Об информации, информатизации и защите информации"</p> <p>г) Закон РФ "О государственной тайне"</p> <p>д) Закон РФ "О коммерческой тайне"</p> <p>е) Закон РФ "О лицензировании отдельных видов</p>	<p>а) Уголовный кодекс РФ</p> <p>б) Конституция РФ</p> <p>в) Закон "Об информации, информатизации и защите информации"</p> <p>г) Закон РФ "О государственной тайне"</p> <p>д) Закон РФ "О коммерческой тайне"</p> <p>е) Закон РФ "О</p>

<p>деятельности"</p> <p>ж) Закон РФ "Об образовании"</p> <p>з) Закон РФ " Об электронной цифровой подписи "</p>	<p>лицензировании отдельных видов деятельности"</p> <p>з) Закон РФ " Об электронной цифровой подписи</p>
<p>10. ВЫБРАТЬ ВАРИАНТЫ ПРАВИЛЬНОГО ОТВЕТА</p> <p><i>Что такое государственная тайна?</i></p> <p>а) Защищаемые государством сведения в области его военной, внешнеполитической, экономической, разведывательной, контрразведывательной и оперативно-розыскной деятельности, распространение которых может нанести ущерб безопасности РФ</p> <p>б) Сведения о состоянии окружающей среды</p> <p>в) Все сведения, которые хранятся в государственных базах данных</p> <p>г) Сведения о состоянии здоровья президента РФ</p> <p>д) Конкретные сведения, в отношении которых компетентные органы и их должностные лица приняли решение об их отнесении к государственной тайне</p>	<p>а) Защищаемые государством сведения в области его военной, внешнеполитической, экономической, разведывательной, контрразведывательной и оперативно-розыскной деятельности, распространение которых может нанести ущерб безопасности РФ</p> <p>д) Конкретные сведения, в отношении которых компетентные органы и их должностные лица приняли решение об их отнесении к государственной тайне</p>
<p>11. ВЫБРАТЬ ВАРИАНТ ПРАВИЛЬНОГО ОТВЕТА</p> <p><i>Что такое коммерческая тайна?</i></p> <p>а) Информация, имеющая действительную или потенциальную коммерческую ценность в силу ее неизвестности третьим лицам</p> <p>б) Информация, к которой нет доступа на законном основании</p> <p>в) Информации, обладатель которой принимает меры к охране ее конфиденциальности</p> <p>г) Информация, содержащая в учредительных документах</p> <p>д) Информация, содержащая в годовых отчетах, бухгалтерских балансах, формах государственных статистических отчетов</p>	<p>а) Информация, имеющая действительную или потенциальную коммерческую ценность в силу ее неизвестности третьим лицам</p> <p>б) Информация, к которой нет доступа на законном основании</p> <p>в) Информации, обладатель которой принимает меры к охране ее конфиденциальности</p>
<p>12. ВЫБРАТЬ ВАРИАНТЫ ПРАВИЛЬНОГО ОТВЕТА</p> <p><i>Согласно Федеральному закону «Об информации, информационных технологиях и защите информации» (№ 149-ФЗ от 27.07.2006 г.) не может быть ограничен доступ к:</i></p> <p>а) нормативным правовым актам, затрагивающим права, свободы и обязанности человека и гражданина, а также устанавливающим правовое положение организаций и полномочия государственных органов, органов местного самоуправления;</p> <p>б) информации о состоянии окружающей среды;</p> <p>в) информации о деятельности государственных органов и органов местного самоуправления, а также об использовании бюджетных, составляющих государственную или служебную тайну;</p>	<p>а) нормативным правовым актам, затрагивающим права, свободы и обязанности человека и гражданина, а также устанавливающим правовое положение организаций и полномочия государственных органов, органов местного самоуправления;</p> <p>б) информации о состоянии окружающей среды;</p>

<p>г) информации, накапливаемой в закрытых фондах в государственных, муниципальных и иных</p> <p>д) информационных системах</p>	
<p>13. ДОПОЛНИТЬ ФРАЗУ</p> <p>Субъект, в полном объеме реализующий полномочия владения, пользования, распоряжения информацией в соответствии с законодательными актами – это</p>	<p>владелец информации</p>
<p>14. ВЫБРАТЬ ВАРИАНТ ПРАВИЛЬНОГО ОТВЕТА</p> <p><i>Защита информации – это</i></p> <p>а) отдельные документы и отдельные массивы документов, документы и массивы документов в информационных системах (библиотеках, архивах, фондах, базах данных и других информационных системах);</p> <p>б) защищенность информации и поддерживающей инфраструктуры от случайных или преднамеренных воздействий естественного или искусственного характера;</p> <p>в) комплекс мероприятий, направленных на обеспечение информационной безопасности;</p> <p>г) процесс сбора, накопления, обработки, хранения, распределения и поиска информации.</p>	<p>в) комплекс мероприятий, направленных на обеспечение информационной безопасности;</p>
<p>15. ВЫБРАТЬ ВАРИАНТ ПРАВИЛЬНОГО ОТВЕТА</p> <p><i>Что такое политика информационной безопасности организации</i></p> <p>а) Набор законов, правил и норм поведения, определяющих, как организация обрабатывает, защищает и распространяет информацию</p> <p>б) Уничтожение, модификация, копирование информации в организации</p> <p>в) Набор административных документов, утвержденных в организации</p> <p>г) Совокупность механизмов компьютерных систем</p> <p>д) Инструкции администраторам по настройке информационных систем</p>	<p>а) Набор законов, правил и норм поведения, определяющих, как организация обрабатывает, защищает и распространяет информацию</p>
<p>16. ВЫБРАТЬ ВАРИАНТЫ ПРАВИЛЬНОГО ОТВЕТА</p> <p><i>Что относится к основным способам физической защиты?</i></p> <p>а) Физическое управление доступом</p> <p>б) Противопожарные меры</p> <p>в) Защита поддерживающей инфраструктуры</p> <p>г) Защита от перехвата данных</p> <p>д) Защита мобильных систем</p> <p>е) Проведение производственной зарядки</p> <p>ж) Проведение соревнований по профессиональному мастерству</p>	<p>а) Физическое управление доступом</p> <p>б) Противопожарные меры</p> <p>в) Защита поддерживающей инфраструктуры</p> <p>г) Защита от перехвата данных</p> <p>д) Защита мобильных систем</p>
<p>17. ВЫБРАТЬ ВАРИАНТ ПРАВИЛЬНОГО ОТВЕТА</p> <p><i>Что такое несанкционированный доступ (нсд)?</i></p> <p>а) Доступ субъекта к объекту в нарушение установленных в системе правил разграничения доступа</p> <p>б) Создание резервных копий в организации</p>	<p>а) Доступ субъекта к объекту в нарушение установленных в системе правил разграничения доступа</p>

<p>в) Правила и положения, выработанные в организации для обхода парольной защиты</p> <p>г) Вход в систему без согласования с руководителем организации</p> <p>д) Удаление не нужной информации</p>	
<p>18. ВЫБРАТЬ ВАРИАНТ ПРАВИЛЬНОГО ОТВЕТА <i>Что такое идентификация?</i></p> <p>а) Процесс распознавания элемента системы, обычно с помощью заранее определенного идентификатора или другой уникальной информации</p> <p>б) Указание на правильность выполненных операций по защите информации</p> <p>в) Определение файлов, которые изменены в информационной системе несанкционированно</p> <p>г) Выполнение процедуры засекречивания файлов</p> <p>д) Процесс периодического копирования информации</p>	<p>а) Процесс распознавания элемента системы, обычно с помощью заранее определенного идентификатора или другой уникальной информации</p>
<p>19. ВЫБРАТЬ ВАРИАНТ ПРАВИЛЬНОГО ОТВЕТА <i>Что такое аутентификация?</i></p> <p>а) Проверка подлинности идентификации пользователя, процесса, устройства или другого компонента системы (обычно осуществляется перед разрешением доступа).</p> <p>б) Нахождение файлов, которые изменены в информационной системе несанкционированно</p> <p>в) Проверка количества переданной и принятой информации</p> <p>г) Определение файлов, из которых удалена служебная информация</p> <p>д) Определение файлов, из которых удалена служебная информация</p>	<p>а) Проверка подлинности идентификации пользователя, процесса, устройства или другого компонента системы (обычно осуществляется перед разрешением доступа).</p>
<p>20. ВЫБРАТЬ ВАРИАНТ ПРАВИЛЬНОГО ОТВЕТА <i>Какими способами обеспечиваются основные уровни антивирусной защиты?</i></p> <p>а) Поиск и уничтожение известных вирусов</p> <p>б) Поиск и уничтожение неизвестных вирусов</p> <p>в) Блокировка проявления вирусов</p> <p>г) Определения адреса отправителя вирусов</p> <p>д) Выявление создателей вирусов</p>	<p>а) Поиск и уничтожение известных вирусов</p> <p>б) Поиск и уничтожение неизвестных вирусов</p> <p>в) Блокировка проявления вирусов</p>

Шкала оценивания:

Тестирование обучающихся проводится после изучения дисциплины в соответствии с настоящей программой и является обязательным для всех студентов. Тесты включены в учебно-методический комплекс дисциплины, размещенный в «Электронной образовательной среде КемГИК».

Тесты включают 20 тестовых заданий. Результаты тестирования оцениваются в баллах в соответствии со следующими критериями:

- 100-90% (20-18 правильных ответов) - «отлично» ;
- 89-75% (17-15 правильных ответов) - «хорошо»;
- 74-60% (14-12 правильных ответов) - «удовлетворительно»;
- ниже 60% (11 и менее правильных ответов) - «неудовлетворительно».

5.2 Методика и критерии оценки результатов обучения по дисциплине

Зачет по дисциплине принимается в форме собеседования (по вопросам), в ходе которого определяется уровень усвоения обучающимися материала, предусмотренного

рабочей программой дисциплины.

Общие правила оценки успеваемости студента в течение семестра

<i>Виды работ</i>	<i>Количество баллов</i>
Выполнение и защита практических работ	Максимум $5 \times 12 = 60$ баллов
Выполнение и защита проекта	Максимум – 20 баллов
Тестирование	Максимум 20 балла
<i>Итого за семестр:</i>	Максимум – 100 баллов

Критерии оценивания

Знания, умения и навыки обучающихся при промежуточной аттестации **в форме зачета** определяются «зачтено», «не зачтено».

«Зачтено» **выставляется, если обучающийся достиг уровней формирования компетенций: продвинутый, повышенный, пороговый** - обучающийся знает курс на уровне лекционного материала, базового учебника, дополнительной учебной, научной и методологической литературы, умеет привести разные точки зрения по излагаемому вопросу.

«Не зачтено» соответствует **нулевому уровню формирования компетенций**; обучающийся имеет пробелы в знаниях основного учебного материала, допускает принципиальные ошибки в выполнении предусмотренных программой заданий.

При использовании 100-балльной шкалы оценивания при промежуточной аттестации, знания, умения и навыки обучающихся определяются в данной шкале и переводятся в оценки «зачтено», «не зачтено».

Шкала перевода баллов в оценки при промежуточной аттестации в форме зачета

Уровень формирования компетенции	Оценка	Минимальное количество баллов	Максимальное количество баллов
Продвинутый, повышенный, пороговый	Зачтено	60	100
Нулевой	Не зачтено	0	59