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

ФОНД ОЦЕНОЧНЫХ СРЕДСТВ

по учебной дисциплине

МЕНЕДЖМЕНТ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ОРГАНИЗАЦИИ

Направление подготовки

46.04.02 «Документоведение и архивоведение»

Профиль подготовки

«Управление документацией в условиях цифровизации общества»

Квалификация (степень) выпускника

Магистр

Форма обучения

Очная, заочная

Год набора - 2022

Составитель: Мишова В.В.

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

Кемерово

1. **Перечень оцениваемых компетенций:**

- Способен разрабатывать и внедрять стратегии цифровой трансформации документированных сфер деятельности организации (ПК-2).
-

2. Планируемые результаты обучения по дисциплине

Обучающийся должен демонстрировать следующие результаты обучения по дисциплине:

знать:

- компоненты концептуальной модели информационной безопасности (З1);
- задачи и функции защиты электронных информационных ресурсов (З2);
- характеристики информационных систем, влияющие на безопасность информации (З3);
- классификацию и характеристику угроз информационной безопасности (З4);
- классификацию преступлений в сфере информационной безопасности (З5);
- нормативно-правовые документы в области защиты информации (З6);
- состав организационных документов обеспечения информационной безопасности (З7);
- классификацию средств программно-технической защиты информации (З8);
- требования к комплексной системе защиты информации в библиотеке (З9);

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 в АБИС (У5);

владеть:

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

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 поверхностью 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.

1. 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. Концептуальные положения защиты информации в информационных системах**			
1.1	Информационная безопасность: определение понятия, состав, назначение	ПК-2	З1, В1	проверка результатов выполнения лабораторной работы
1.2	Информационная система как объект защиты	ПК-2	З2, З3, В1	проверка результатов выполнения лабораторной работы
1.3	Угрозы информационной безопасности в информационных системах	ПК-2	З4, З5, У1, В2, В1	проверка результатов выполнения лабораторной работы
2	**Раздел 2. Направления защиты информации в документационном обеспечении управления и архивном деле**			
2.1	Правовое обеспечение информационной безопасности	ПК-2	З6, У2, В1	проверка результатов выполнения лабораторной работы
2.2	Организационное обеспечение информационной безопасности	ПК-2	З7, У3, В3	проверка результатов выполнения лабораторной работы

2.3	Программно-техническое обеспечение информационной безопасности	ПК-2	З8, У4, В4	проверка результатов выполнения лабораторной работы, тестирование
2.4	Комплексная система защиты информации	ПК-2	З9, У5, В5	реализация учебного проекта

2. Оценочные средства по дисциплине для текущего контроля

4.3. Лабораторное работы

В ходе освоения учебной дисциплины предусмотрено 12 лабораторных работ (28 часов). Описания лабораторных работ представлены в электронном учебно-методическом комплексе дисциплины, размещенном на сайте «Электронная образовательная среда КемГИК»).

Критерии оценивания:

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

4.5. Тематика учебных исследовательских проектов

1. Разработать модель информационной безопасности областной архива.
2. Разработать модель информационной безопасности библиотеки.
3. Разработать модель информационной безопасности организации с электронным документооборотом.
4. Разработать модель информационной безопасности городского архива.
5. Разработать модель информационной безопасности администрации поселка N.

Критерии оценивания:

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
Критерии оценки проекта	
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
Критерии оценки выступлений	
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 промежуточной аттестации и шкала оценивания

5.1 СПИСОК ВОПРОСОВ ДЛЯ ПРОВЕДЕНИЯ ПРОМЕЖУТОЧНОЙ АТТЕСТАЦИИ И ПРОВЕРКИ СФОРМИРОВАННОСТИ КОМПЕТЕНЦИЙ

Номер вопроса	***Правильный ответ***
1. ВЫБРАТЬ ВАРИАНТЫ ПРАВИЛЬНОГО ОТВЕТА *Какие существуют основные уровни обеспечения защиты информации?* а) Законодательный б) Организационно-административный в) Программно-технический (аппаратный) г) Физический д) Вероятностный е) Распределительный	законодательный (а), организационно-административный (б), программно-технический (аппаратный) (в), физический (г)
2. ВЫБРАТЬ ВАРИАНТЫ ПРАВИЛЬНОГО ОТВЕТА *Какие основные свойства информации и систем обработки информации необходимо поддерживать, обеспечивая информационную безопасность?* а) Доступность б) Целостность в) Конфиденциальность г) Управляемость д) Сложность	доступность (а), целостность (б), конфиденциальность (в)
3. ВЫБРАТЬ ВАРИАНТ ПРАВИЛЬНОГО ОТВЕТА *Что такое доступность информации?* а) Свойство системы, в которой циркулирует информация,	свойство системы, в которой циркулирует информация,

характеризующееся способностью обеспечивать своевременный беспрепятственный доступ к информации субъектов, имеющих на это надлежащие полномочия б) Свойство системы, обеспечивать беспрепятственный доступ к информации любых субъектов в) Свойство системы, обеспечивать закрытый доступ к информации любых субъектов г) Свойство информации, заключающееся в легкости ее несанкционированного получения и дальнейшего распространения (несанкционированного копирования)	характеризующееся способностью обеспечивать своевременный беспрепятственный доступ к информации субъектов, имеющих на это надлежащие полномочия (а)
4. ВЫБРАТЬ ВАРИАНТ ПРАВИЛЬНОГО ОТВЕТА *Что такое целостность информации?* а) Свойство информации, заключающееся в ее существовании в неискаженном виде (неизменном по отношению к некоторому фиксированному ее состоянию) б) Свойство информации, заключающееся в возможности ее изменения любым субъектом в) Свойство информации, заключающееся в возможности изменения только единственным пользователем г) Свойство информации, заключающееся в ее существовании в виде единого набора файлов	свойство информации, заключающееся в ее существовании в неискаженном виде (неизменном по отношению к некоторому фиксированному ее состоянию) (а)
5. ВЫБРАТЬ ВАРИАНТ ПРАВИЛЬНОГО ОТВЕТА *Что такое конфиденциальность информации?* 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 б) Свойство информации, заключающееся в ее существовании в неискаженном виде (неизменном по отношению к некоторому фиксированному ее состоянию) в) Свойство информации, заключающееся в ее существовании в виде не защищенного паролем набора г) Свойство информации, заключающееся в ее шифрования д) Свойство информации, заключающееся в ее принадлежности к определенному набору	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 (а)
6. ВЫБРАТЬ ВАРИАНТЫ ПРАВИЛЬНОГО ОТВЕТА *Что относится к угрозам информационной безопасности?* а) Потенциально возможное событие, действие, процесс или явление, которое может привести к нарушению конфиденциальности, целостности, доступности информации, а также неправомерному ее тиражированию б) Классификация информации в) Стихийные бедствия и аварии (наводнение, ураган, землетрясение, пожар и т.п.) г) Сбои и отказы оборудования (технических средств) АС д) Ошибки эксплуатации (пользователей, операторов и другого персонала) е) Преднамеренные действия нарушителей и злоумышленников (обиженных лиц из числа персонала,	потенциально возможное событие, действие, процесс или явление, которое может привести к нарушению конфиденциальности, целостности, доступности информации, а также неправомерному ее тиражированию (а); стихийные бедствия и аварии (наводнение, ураган, землетрясение, пожар и т.п.)(в); сбои и

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

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

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

18. ВЫБРАТЬ ВАРИАНТ ПРАВИЛЬНОГО ОТВЕТА *Что такое идентификация?* а) Процесс распознавания элемента системы, обычно с помощью заранее определенного идентификатора или другой уникальной информации б) Указание на правильность выполненных операций по защите информации в) Определение файлов, которые изменены в информационной системе несанкционированно г) Выполнение процедуры засекречивания файлов д) Процесс периодического копирования информации	процесс распознавания элемента системы, обычно с помощью заранее определенного идентификатора или другой уникальной информации (а)
19. ВЫБРАТЬ ВАРИАНТ ПРАВИЛЬНОГО ОТВЕТА *Что такое аутентификация?* а) Проверка подлинности идентификации пользователя, процесса, устройства или другого компонента системы (обычно осуществляется перед разрешением доступа). б) Нахождение файлов, которые изменены в информационной системе несанкционированно в) Проверка количества переданной и принятой информации г) Определение файлов, из которых удалена служебная информация д) Определение файлов, из которых удалена служебная информация	проверка подлинности идентификации пользователя, процесса, устройства или другого компонента системы (обычно осуществляется перед разрешением доступа) (а)
20. ВЫБРАТЬ ВАРИАНТ ПРАВИЛЬНОГО ОТВЕТА *Какими способами обеспечиваются основные уровни антивирусной защиты?* а) Поиск и уничтожение известных вирусов б) Поиск и уничтожение неизвестных вирусов в) Блокировка проявления вирусов г) Определения адреса отправителя вирусов д) Выявление создателей вирусов	поиск и уничтожение известных вирусов (а), поиск и уничтожение неизвестных вирусов (б), блокировка проявления вирусов (в)

Шкала оценивания:

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

5.2. Вопросы к зачету

1. Информационная безопасность: понятие, назначение
2. Состав концептуальной модели информационной безопасности
3. Доступность, целостность и конфиденциальность информации
4. Проблемы защиты информационных систем
5. Характеристики информационных систем, влияющие на безопасность информации
6. Классификация и характеристика угроз информационной безопасности
7. Причины и источники случайных воздействий на информационные системы
8. Причины и источники преднамеренных воздействий на информационные системы
9. Классификация преступлений в сфере информационной безопасности
10. Основные положения государственной политики обеспечения информационной безопасности РФ
11. Государственная тайна: понятие, средства защиты государственной тайны

12. Конфиденциальная информация: понятие, средства защиты конфиденциальной информации
13. Персональные данные: понятие, средства защиты персональных данных
14. Цели, задачи, содержание административного уровня обеспечения информационной безопасности.
15. Цели, задачи, содержание процедурного уровня обеспечения информационной безопасности.
16. Политика безопасности: определение, направления разработки
17. Классификация средств технической защиты информации.
18. Классификация средств программной защиты информации.
19. Компьютерные вирусы: классификация, деструктивные возможности
20. Виды антивирусных программ. Факторы, определяющие качество антивирусных программ
21. Правила защиты от компьютерных вирусов, получаемых не из вычислительных сетей.
22. Идентификация и аутентификация пользователей

Критерии оценивания

Общие правила оценки успеваемости студента в течение семестра

Виды работ	*Количество баллов*
Выполнение и защита лабораторных работ	Максимум 5 × 12= 60 баллов
Выполнение и защита проекта	Максимум – 20 баллов
Тестирование	Максимум 20 балла
Итого за семестр:	Максимум – 100 баллов

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

Оценка **«зачтено»** выставляется обучающемуся в ходе *собеседования* при выполнении следующих критериев: обучающийся знает курс на уровне лекционного материала, базовых учебных пособий, дополнительной учебной, научной литературы, умеет привести разные точки зрения по излагаемому вопросу; дает логически последовательные, содержательные, правильные ответы на вопросы; владеет терминологическим аппаратом; допускаются неточности при ответе, которые при наводящих вопросах студент исправляет.

«Не зачтено» соответствует **нулевому уровню формирования компетенций:** обучающийся имеет пробелы в знаниях основного учебного материала, не знает значительной части программного материала, допускает принципиальные ошибки в выполнении предусмотренных программой заданий либо не выполнил практические задания.

«Зачтено» выставляется, если обучающийся достиг **уровней формирования компетенций: продвинутый, повышенный, пороговый.**

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