

Документ подписан простой электронной подписью

Информация о владельце:

ФИО: Таскаев Сергей Васильевич

Должность: Ректор

Дата подписания: 15.09.2025 11:03:21

Уникальный программный ключ:

04c19ed8bfb98f3b6cb77a48009a878808522525

МИНОБРНАУКИ РОССИИ

Федеральное государственное бюджетное образовательное

учреждение высшего образования

«Челябинский государственный университет» (ФГБОУ ВО «ЧелГУ»)

Математический факультет

Кафедра компьютерной безопасности и прикладной алгебры

Фонд оценочных средств по дисциплине «Тестирование компьютерных систем на проникновения»

по специальности 10.05.01 Компьютерная безопасность

специализации № 6 «Информационно-аналитическая и техническая экспертиза компьютерных систем»

Версия документа - 1	стр. 1	Первый экземпляр _____	КОПИЯ № _____
----------------------	--------	------------------------	---------------

**Фонд оценочных средств
для промежуточной аттестации
по дисциплине**

Тестирование компьютерных систем на проникновения

Направление подготовки (специальность)
10.05.01 Компьютерная безопасность

Направленность (профиль)
специализация № 6 «Информационно-аналитическая и техническая
экспертиза компьютерных систем»

Присваиваемая квалификация
специалист по защите информации

Форма обучения
очная

Челябинск 2025 г.



МИНОБРНАУКИ РОССИИ
Федеральное государственное бюджетное образовательное
учреждение высшего образования
«Челябинский государственный университет» (ФГБОУ ВО «ЧелГУ»)
Математический факультет
Кафедра компьютерной безопасности и прикладной алгебры

Фонд оценочных средств по дисциплине «Тестирование компьютерных систем на проникновения»
по специальности 10.05.01 Компьютерная безопасность
специализации № 6 «Информационно-аналитическая и техническая экспертиза компьютерных систем»

Версия документа - 1

стр. 2

Первый экземпляр _____

КОПИЯ № _____

Содержание

1. Паспорт фонда оценочных средств
2. Перечень формируемых компетенций
 - 2.1. Компетенции, закреплённые за дисциплиной
3. Содержание оценочных средств по дисциплине
 - 3.1. Виды оценочных средств
 - 3.2. Содержание оценочных средств
4. Порядок проведения и критерии оценивания промежуточной аттестации
 - 4.1. Порядок проведения промежуточной аттестации
 - 4.2. Критерии оценивания промежуточной аттестации по видам оценочных средств
 - 4.3. Результаты промежуточной аттестации и уровни сформированности компетенций



МИНОБРНАУКИ РОССИИ
Федеральное государственное бюджетное образовательное
учреждение высшего образования
«Челябинский государственный университет» (ФГБОУ ВО «ЧелГУ»)
Математический факультет
Кафедра компьютерной безопасности и прикладной алгебры

Фонд оценочных средств по дисциплине «Тестирование компьютерных систем на проникновения»
по специальности 10.05.01 Компьютерная безопасность
специализации № 6 «Информационно-аналитическая и техническая экспертиза компьютерных систем»

Версия документа - 1

стр. 3

Первый экземпляр _____

КОПИЯ № ____

1. ПАСПОРТ ФОНДА ОЦЕНОЧНЫХ СРЕДСТВ

Специальность 10.05.01 Компьютерная безопасность.

Специализация № 6 «Информационно-аналитическая и техническая экспертиза компьютерных систем».

Дисциплина: **Тестирование компьютерных систем на проникновения.**

Семестр (семестры) изучения: 9 семестр.

Форма (формы) промежуточной аттестации: экзамен 9 семестр.

Используется балльно-рейтинговая система для оценивания результатов.

2. ПЕРЕЧЕНЬ ФОРМИРУЕМЫХ КОМПЕТЕНЦИЙ

2.1. Компетенции, закреплённые за дисциплиной

Изучение дисциплины «Тестирование компьютерных систем на проникновения» направлено на формирование следующих компетенций:

Коды компетенции согласно ФГОС (ОПОП ВО)	Содержание компетенций согласно ФГОС (ОПОП ВО)	Индикаторы достижения компетенции согласно ОПОП	Перечень планируемых результатов обучения по дисциплине
1	2	3	4
ПК-2	Способен проводить мониторинг защищенности компьютерных систем	ПК-2.1. Обладает знаниями о принципах построения систем обнаружения компьютерных атак; о методах обработки данных мониторинга безопасности компьютерных систем и сетей; о порядке создания и структура отчета, создаваемого по результатам проверок; о способах обнаружения и нейтрализации последствий вторжений в компьютерные системы; о нормативных правовых актах в области защиты информации; о руководящих и методических документах уполномоченных федеральных органов исполнительной власти по защите информации. ПК-2.2. Демонстрирует умения: формализовывать задачу управления безопасностью компьютерных систем; применять инструментальные средства проведения мониторинга защищенности компьютерных систем;	Знать: – этапы проведения тестирования компьютерных систем на проникновение; – теоретические основы компьютерных атак, моделируемых в рамках проведения экспериментов по проникновению в компьютерные системы; – принципы работы сканеров безопасности и методику проверки получаемых ими сведений; – правила документирования и построения отчетов по результатам проводимых тестов на проникновение. Уметь: – использовать сканеры информационной безопасности и проводить оценку, получаемых ими сведений; – моделировать современные компьютерные атаки, представляющие актуальные угрозы



МИНОБРНАУКИ РОССИИ
Федеральное государственное бюджетное образовательное
учреждение высшего образования
«Челябинский государственный университет» (ФГБОУ ВО «ЧелГУ»)
Математический факультет
Кафедра компьютерной безопасности и прикладной алгебры

Фонд оценочных средств по дисциплине «Тестирование компьютерных систем на проникновения»
по специальности 10.05.01 Компьютерная безопасность
специализации № 6 «Информационно-аналитическая и техническая экспертиза компьютерных систем»

Версия документа - 1

стр. 4

Первый экземпляр _____

КОПИЯ № _____

		<p>Применять методы анализа защищенности компьютерных систем и сетей; структурировать аналитическую информацию для включения в отчет.</p> <p>ПК-2.3. Имеет практический опыт (навыки): выполнение анализа защищенности компьютерных систем с использованием сканеров безопасности; выполнение анализа защищенности сетевых сервисов с использованием средств автоматического реагирования на попытки несанкционированного доступа к ресурсам компьютерных систем и сетей; составление отчетов по результатам проверок.</p>	<p>информационной безопасности для компьютерных систем;</p> <ul style="list-style-type: none">– детектировать средства обнаружения компьютерных вторжений и предотвращения утечек информации;– использовать приемы обхода IDS, IPS, DLP-систем, антивирусного программного обеспечения и криптографических протоколов, применяемых для защиты компьютерных систем;– проводить оценку конфигурации средств защиты информации и давать рекомендации по ее корректировке. <p>Владеть:</p> <ul style="list-style-type: none">– практическими навыками проведения тестирования компьютерных систем на проникновение и подготовки по их результатам соответствующих отчетов.
--	--	--	--



МИНОБРНАУКИ РОССИИ
Федеральное государственное бюджетное образовательное
учреждение высшего образования
«Челябинский государственный университет» (ФГБОУ ВО «ЧелГУ»)
Математический факультет
Кафедра компьютерной безопасности и прикладной алгебры

Фонд оценочных средств по дисциплине «Тестирование компьютерных систем на проникновения»
по специальности 10.05.01 Компьютерная безопасность
специализации № 6 «Информационно-аналитическая и техническая экспертиза компьютерных систем»

Версия документа - 1

стр. 5

Первый экземпляр _____

КОПИЯ № _____

3. СОДЕРЖАНИЕ ОЦЕНОЧНЫХ СРЕДСТВ ПО ДИСЦИПЛИНЕ

3.1. Виды оценочных средств

№ п/п	Код компетенции / планируемые результаты обучения	Контролируемые темы/ разделы	Наименование оценочного средства для текущего контроля	Наименование оценочного средства на промежуточной аттестации/№ задания
1.	ПК-2	Раздел 1. Методика проведения тестирования компьютерных систем	Вопросы для устного опроса № 1-5.	Вопросы к экзамену № 1-5.
2.	ПК-2	Раздел 2. Сбор информации	Вопросы для устного опроса № 6-11. Самостоятельная работа № 2. Лабораторная работа № 1.	Вопросы к экзамену № 6-9.
3.	ПК-2	Раздел 3. Сканирование компьютерных систем	Вопросы для устного опроса № 12-19. Самостоятельная работа № 1. Лабораторная работа № 2.	Вопросы к экзамену № 10-11.
4.	ПК-2	Раздел 4. Эксплуатация уязвимостей программного обеспечения	Вопросы для устного опроса № 20-29. Лабораторные работы № 3-4.	Вопросы к экзамену № 12-14.
5.	ПК-2	Раздел 5. Проведение экспериментов по оценке защищенности вычислительных систем	Вопросы для устного опроса № 30-45. Лабораторные работы № 5-10.	Вопросы к экзамену № 16-23.
6.	ПК-2	Раздел 6. Оценка защищенности компьютерных систем, выработка рекомендаций	Вопросы для устного опроса № 1-3, 46. Лабораторная работа № 11.	Вопросы к экзамену № 1-3, 24.

Типовые задания, критерии и показатели оценивания в рамках текущего контроля представлены в рабочей программе дисциплины (модуля). Полные комплекты оценочных средств и контрольно-измерительных материалов хранятся на кафедре.



МИНОБРНАУКИ РОССИИ
Федеральное государственное бюджетное образовательное
учреждение высшего образования
«Челябинский государственный университет» (ФГБОУ ВО «ЧелГУ»)
Математический факультет
Кафедра компьютерной безопасности и прикладной алгебры

Фонд оценочных средств по дисциплине «Тестирование компьютерных систем на проникновения»
по специальности 10.05.01 Компьютерная безопасность
специализации № 6 «Информационно-аналитическая и техническая экспертиза компьютерных систем»

Версия документа - 1

стр. 6

Первый экземпляр _____

КОПИЯ № _____

3.2. Содержание оценочных средств

3.2.1. Вопросы для устного опроса для текущей аттестации

1. Этапы тестирования компьютерных систем на проникновение.
2. Виды и классификации тестирований компьютерных систем на проникновение.
3. Black box, White box, Black hat, White hat.
4. Понятие этичного взлома.
5. Правовые основы проведения теста на проникновение.
6. Понятие и назначение «Open source intelligence».
7. Lo-tech OSINT.
8. Hi-tech OSINT.
9. Общее понятие футпринтинга.
10. Принципы технологии «google hacking database».
11. Методы анализа метаданных.
12. Методы сканирования портов.
13. SYN-сканирование.
14. ACK-сканирование.
15. XMAS-сканирование.
16. FIN-сканирование.
17. UDP-сканирование.
18. Window-сканирование.
19. Способы идентификации приложений, детектирование уязвимостей.
20. Алгоритмы функционирования антивирусных средств.
21. Проактивная защита.
22. Реактивная защита.
23. Виртуализация окружения.
24. Эмуляция кода.
25. Полиморфный программный код.
26. Метаморфный программный код.
27. Шифрование программного кода.
28. Методы обхода средств антивирусной защиты, сетевых экранов, систем обнаружений вторжений.
29. Эксплойт.
30. Классификация компьютерных атак.
31. Сетевые атаки на канальный уровень стека протоколов TCP/IP.
32. Сетевые атаки на сетевой уровень стека протоколов TCP/IP.
33. Сетевые атаки на транспортный уровень стека протоколов TCP/IP.



МИНОБРНАУКИ РОССИИ
Федеральное государственное бюджетное образовательное
учреждение высшего образования
«Челябинский государственный университет» (ФГБОУ ВО «ЧелГУ»)
Математический факультет
Кафедра компьютерной безопасности и прикладной алгебры

Фонд оценочных средств по дисциплине «Тестирование компьютерных систем на проникновения»
по специальности 10.05.01 Компьютерная безопасность
специализации № 6 «Информационно-аналитическая и техническая экспертиза компьютерных систем»

Версия документа - 1

стр. 7

Первый экземпляр _____

КОПИЯ № _____

34. Атаки на протоколы маршрутизации.
35. Протокол DHCP.
36. Истощение DHCP-сервера.
37. DNS.
38. DNS-спуфинг.
39. Шторм ложных DNS-запросов.
40. Методы целевого внедрения специального программного обеспечения.
41. Атака Strip-SSL.
42. Механизм защиты HSTS.
43. HSTS спуфинг.
44. Алгоритм работы WPA2.
45. Атака деаутентификации WPA2.
46. Документальное оформление теста на проникновение

3.2.2. Перечень самостоятельных работ

1. Разработка сетевого сканера.
2. Использование технологии OSINT в открытых телекоммуникационных сетях.

3.2.3. Перечень лабораторных работ

1. Сбор информации в открытых телекоммуникационных сетях.
2. Использование библиотеки "scapy" для проведения различных видов сканирования сетевых портов.
3. Использование программного обеспечения «Metasploit Framework».
4. Использование дополнительных модулей «Metasploit Framework».
5. Прослушивание и модификация сетевого трафика.
6. Подавление в сети DHCP-сервера.
7. Атака на клиентское приложение.
8. Атака «stripssl» на протокол HTTPS.
9. Анализ сетевого трафика программой Interceptor-NG.
10. Атака на беспроводную сеть.
11. Отчет о проведении тестирования компьютерной системы на проникновение.

3.2.4. Перечень вопросов к экзамену

1. Этапы тестирования компьютерных систем на проникновение.
2. Виды и классификации тестирований компьютерных систем на



МИНОБРНАУКИ РОССИИ
Федеральное государственное бюджетное образовательное
учреждение высшего образования
«Челябинский государственный университет» (ФГБОУ ВО «ЧелГУ»)
Математический факультет
Кафедра компьютерной безопасности и прикладной алгебры

Фонд оценочных средств по дисциплине «Тестирование компьютерных систем на проникновения»
по специальности 10.05.01 Компьютерная безопасность
специализации № 6 «Информационно-аналитическая и техническая экспертиза компьютерных систем»

Версия документа - 1

стр. 8

Первый экземпляр _____

КОПИЯ № _____

проникновение.

3. Black box, White box, Black hat, White hat.
4. Понятие этичного взлома.
5. Правовые основы проведения теста на проникновение.
6. Понятие и назначение «Open source intelligence».
7. Общее понятие футпринтинга.
8. Принципы технологии «google hacking database».
9. Методы анализа метаданных.
10. Методы сканирования портов.
11. Способы идентификации приложений, детектирование уязвимостей.
12. Алгоритмы функционирования антивирусных средств.
13. Методы обхода средств антивирусной защиты, сетевых экранов, систем обнаружений вторжений.
14. Общая схема применения эксплойта.
15. Классификация компьютерных атак.
16. Сетевые атаки на канальный уровень стека протоколов TCP/IP.
17. Сетевые атаки на сетевой уровень стека протоколов TCP/IP.
18. Сетевые атаки на транспортный уровень стека протоколов TCP/IP.
19. Атаки на протоколы маршрутизации.
20. Уязвимости DHCP-протокола.
21. Атаки на службу DNS.
22. Методы целевого внедрения специального программного обеспечения.
23. Атака Strip-SSL.
24. Документальное оформление теста на проникновение.

Полные тексты лабораторных работ и задания выложены на сетевом диске кафедры компьютерной безопасности и прикладной алгебры DC1\doc\.



МИНОБРНАУКИ РОССИИ
Федеральное государственное бюджетное образовательное
учреждение высшего образования
«Челябинский государственный университет» (ФГБОУ ВО «ЧелГУ»)
Математический факультет
Кафедра компьютерной безопасности и прикладной алгебры

Фонд оценочных средств по дисциплине «Тестирование компьютерных систем на проникновения»
по специальности 10.05.01 Компьютерная безопасность
специализации № 6 «Информационно-аналитическая и техническая экспертиза компьютерных систем»

Версия документа - 1

стр. 9

Первый экземпляр _____

КОПИЯ № ____

4. ПОРЯДОК ПРОВЕДЕНИЯ И КРИТЕРИИ ОЦЕНИВАНИЯ ПРОМЕЖУТОЧНОЙ АТТЕСТАЦИИ

4.1. Порядок проведения промежуточной аттестации

В течение семестра студент должен выполнить одиннадцать лабораторных работ, каждая из которых оценивается в 5 баллов.

Максимальный балл за лабораторную работу – 5 баллов.

Максимальный балл за лабораторные работы в семестре – 55 баллов.

Также необходимо выполнить две самостоятельные работы.

Максимальный балл за самостоятельную работу – 5 баллов.

Допуском до проведения экзамена являются сданные студентом лабораторные и самостоятельные работы в течение семестра. Экзамен проводится в один этап, на котором студент отвечает на два теоретических вопроса. Продолжительность – 30 минут.

Максимальный балл за ответ на теоретический вопрос – 15 баллов.

Сводная таблица рейтинга успеваемости

№	Перечень контрольных мероприятий в семестре	Максимальное кол-во баллов
1	Лабораторная работа №1-11	11x5=55
2	Самостоятельная работа № 1,2	2x5=10
3	Посещаемость (все занятия)	5
4	Экзамен (теоретический вопрос)	2x15=30
	Итого	100

4.2. Критерии оценивания промежуточной аттестации по видам оценочных средств.

4.2.1 Критерии оценивания теоретического вопроса

Максимальный баллы за ответ на теоретический вопрос – 15 баллов.

Оценка	Отлично/зачтено	Хорошо/зачтено	Удовлетворительно /зачтено	Неудовлетворительно/не зачтено
Баллы	13-15 баллов	9-12 баллов	6-8 баллов	0-5 баллов
Критерии оценивания вопроса: 1. Полнота изложения теоретического материала.	Студентом дан полный, в логической последовательности развернутый ответ на поставленный вопрос, в котором он	Студентом дан развернутый ответ на поставленный вопрос, в котором студент демонстрирует знания,	Студентом дан ответ, свидетельствующий, в основном, о знании процессов изучаемой дисциплины, отличающийся	Студентом дан ответ, который содержит ряд серьезных неточностей, обнаруживающий незнание процессов изучаемой



МИНОБРНАУКИ РОССИИ
Федеральное государственное бюджетное образовательное
учреждение высшего образования
«Челябинский государственный университет» (ФГБОУ ВО «ЧелГУ»)
Математический факультет
Кафедра компьютерной безопасности и прикладной алгебры

Фонд оценочных средств по дисциплине «Тестирование компьютерных систем на проникновения»
по специальности 10.05.01 Компьютерная безопасность
специализации № 6 «Информационно-аналитическая и техническая экспертиза компьютерных систем»

Версия документа - 1	стр. 10	Первый экземпляр _____	КОПИЯ № _____
----------------------	---------	------------------------	---------------

2. Правильность и/или аргументированность изложения (последовательность действий) 3. Самостоятельность ответа	продемонстрировал знания предмета в полном объеме учебной программы, достаточно глубоко осмысливает дисциплину, самостоятельно, и исчерпывающе отвечает на дополнительные вопросы, приводит собственные примеры по проблематике поставленного вопроса.	приобретенные на лекционных и семинарских занятиях, а также полученные посредством изучения обязательных учебных материалов по курсу, дает аргументированные ответы, приводит примеры, логичность и последовательно выстраивает ответ. Однако, допускает неточность в ответе.	недостаточной глубиной и полнотой раскрытия темы, знанием основных вопросов теории, слабо сформированными навыками анализа явлений, процессов, недостаточным умением давать аргументированные ответы и приводить примеры, недостаточной логичностью и последовательностью ответа.	предметной области, отличающийся неглубоким раскрытием темы, незнанием основных вопросов теории, несформированными навыками анализа явлений, процессов, неумением давать аргументированные ответы, отсутствием логичности и последовательности. Выводы поверхностны. Студент не способен ответить на вопросы даже при дополнительных наводящих вопросах преподавателя.
Уровень освоения проверяемых компетенций	высокий	средний	базовый	недостаточный

4.2.2. Критерии оценки лабораторной работы

Максимальный балл за лабораторные работы за семестр – 55 баллов.

5 баллов - лабораторная работа выполнена полно и правильно в соответствии с заданием, вывод сделан самостоятельно, технически правильным языком, даны верные ответы на контрольные вопросы, по заданию преподавателя продемонстрированы дополнительные действия в рамках тематики работы;

4 балла – лабораторная работа выполнена полно и правильно в соответствии с заданием, вывод сделан самостоятельно, технически правильным языком, даны не полные ответы на контрольные вопросы, по заданию преподавателя продемонстрированы дополнительные действия в рамках тематики работы;

3 балла – лабораторная работа выполнена полно и правильно в соответствии с заданием, вывод сделан самостоятельно, технически правильным языком, даны не полные ответы на контрольные вопросы, по заданию преподавателя не продемонстрированы дополнительные действия в рамках тематики работы;

2 балла – лабораторная работа выполнена неполно, вывод не сделан, даны не полные ответы на контрольные вопросы, по заданию преподавателя не продемонстрированы дополнительные действия в рамках тематики работы;

1 балл – при выполнении лабораторной работы обучающимся допущены существенные ошибки по содержанию учебного материала, работа выполнена с нарушением, допущены грубые ошибки, на контрольные вопросы даны не верные ответы.

0 баллов – не выполнена лабораторная работа.



МИНОБРНАУКИ РОССИИ
Федеральное государственное бюджетное образовательное
учреждение высшего образования
«Челябинский государственный университет» (ФГБОУ ВО «ЧелГУ»)
Математический факультет
Кафедра компьютерной безопасности и прикладной алгебры

Фонд оценочных средств по дисциплине «Тестирование компьютерных систем на проникновения»
по специальности 10.05.01 Компьютерная безопасность
специализации № 6 «Информационно-аналитическая и техническая экспертиза компьютерных систем»

Версия документа - 1

стр. 11

Первый экземпляр _____

КОПИЯ № _____

4.2.3. Критерии оценки самостоятельной работы

Максимальный балл за самостоятельные работы за семестр –10 баллов.

5 баллов – самостоятельная работа выполнена полно и правильно в соответствии с заданием, вывод сделан самостоятельно, технически правильным языком, даны верные ответы на контрольные вопросы, по заданию преподавателя продемонстрированы дополнительные действия в рамках тематики работы;

4 балла – самостоятельная работа выполнена полно и правильно в соответствии с заданием, вывод сделан самостоятельно, технически правильным языком, даны не полные ответы на контрольные вопросы, по заданию преподавателя продемонстрированы дополнительные действия в рамках тематики работы;

3 балла – самостоятельная работа выполнена полно и правильно в соответствии с заданием, вывод сделан самостоятельно, технически правильным языком, даны не полные ответы на контрольные вопросы, по заданию преподавателя не продемонстрированы дополнительные действия в рамках тематики работы;

2 балла – лабораторная работа выполнена неполно, вывод не сделан, даны не полные ответы на контрольные вопросы, по заданию преподавателя не продемонстрированы дополнительные действия в рамках тематики работы;

1 балл – при выполнении самостоятельной работы обучающимся допущены существенные ошибки по содержанию учебного материала, работа выполнена с нарушением, допущены грубые ошибки, на контрольные вопросы даны не верные ответы.

0 баллов – не выполнена самостоятельная работа.

4.3. Результаты промежуточной аттестации и уровни сформированности компетенций

При подведении итогов учитываются результаты текущей аттестации. Полученные за текущую аттестацию баллы суммируются с баллами, полученными за каждый этап при прохождении промежуточной аттестации.

Для экзамена:

0-60 баллов – неудовлетворительно (2);

61-74 баллов – удовлетворительно (3);

75-90 баллов – хорошо (4);

91-100 баллов – отлично (5).

Особенности проведения процедуры оценивания результатов обучения инвалидов и лиц с ограниченными возможностями здоровья обозначены в рабочей программе дисциплины (модуля).

Уровни сформированности компетенций определяется следующим образом

Оценка	Отлично/	Хорошо/	Удовлетворитель	Неудовлетворите
--------	----------	---------	-----------------	-----------------



МИНОБРНАУКИ РОССИИ
Федеральное государственное бюджетное образовательное
учреждение высшего образования
«Челябинский государственный университет» (ФГБОУ ВО «ЧелГУ»)
Математический факультет
Кафедра компьютерной безопасности и прикладной алгебры

Фонд оценочных средств по дисциплине «Тестирование компьютерных систем на проникновения»
по специальности 10.05.01 Компьютерная безопасность
специализации № 6 «Информационно-аналитическая и техническая экспертиза компьютерных систем»

Версия документа - 1

стр. 12

Первый экземпляр _____

КОПИЯ № _____

	зачтено	зачтено	но/ зачтено	льно/ незачтено
Баллы	91-100 баллов	75-90 баллов	60-74 баллов	0-59 баллов
Уровень освоения проверяемых компетенций	высокий	средний	базовый	недостаточный

Уровни сформированности компетенций определяется следующим образом:

1. **Высокий уровень сформированности компетенций** соответствует оценке «Отлично»:
 - предполагает формирование компетенций на высоком уровне, готовность к самостоятельной профессиональной деятельности,
 - студент способен аргументировать собственную точку зрения по дискуссионным вопросам дисциплины, решать ситуационные задачи, формулировать собственные выводы.
2. **Средний уровень** соответствует оценке «Хорошо»:
 - предполагает формирование компетенций на достаточном уровне,
 - студент способен давать развернутые ответы на теоретические и практические вопросы дисциплины на уровне не ниже оценки «Хорошо».
3. **Базовый уровень** соответствует оценке «Удовлетворительно»:
 - предполагает формирование компетенций на начальном уровне,
 - студент способен давать ответы на теоретические и практические вопросы дисциплины на уровне не ниже оценки «Удовлетворительно»,
 - студент способен отвечать на вопросы в закрытой форме. Количество правильных ответов – не менее 50%.
4. **Низкий уровень** соответствует оценке «Неудовлетворительно».

