МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ
Федеральное государственное автономное образовательное учреждение высшего образования
«СЕВЕРО-КАВКАЗСКИЙ ФЕДЕРАЛЬНЫЙ УНИВЕРСИТЕТ»

УТВЕРЖДАЮ
И.о. декана факультета математики
и компьютерных наук имени
профессора Н.И. Червякова
Т.А. Гробова
Ф.И.О.

ФОНД ОЦЕНОЧНЫХ СРЕДСТВ ПО ДИСЦИПЛИНЕ

Кибербезопасность мультиагентных робототехнических систем

Направление подготовки	10.04.01 Информационная безопасность
Направленность (профиль)	Информационная безопасность киберфизических систем
Год начала обучения	2026
Форма обучения	очная
Реализуется в семестре	2

Ставрополь 2026 г.

Введение

1. Назначение: данный фонд оценочных предназначен для оценивания уровня сформированности компетенций при проведении текущего контроля успеваемости и промежуточной аттестации студентов, обучающихся по направлению подготовки 10.04.01 Информационная безопасность, направленность (профиль) «Информационная безопасность киберфизических систем» по дисциплине «Кибербезопасность мультиагентных робототехнических систем».

2. Фонд оценочных средств текущего контроля и промежуточной аттестации на основе рабочей программы дисциплины «Кибербезопасность мультиагентных робототехнических систем» в соответствии с образовательной программой 10.04.01 Информационная безопасность, направленность (профиль) «Информационная безопасность» по дисциплине «Кибербезопасность мультиагентных робототехнических систем».

3. Разработчик: к.т.н., доцент Рачков Валерий Евгеньевич, доцент кафедры организации и технологии защиты информации.

4. Проведена экспертиза ФОС.
Члены экспертной группы:
Председатель: Петренко В.И., заведующий кафедрой
Члены экспертной группы: Жук А.П., профессор кафедры
Минкина Т.В., доцент кафедры

Представитель организации-работодателя Демурчев Н.Г., директор ООО «Инфоком-С»

Экспертное заключение: фонд оценочных средств соответствует ОП ВО по направлению подготовки 10.04.01 Информационная безопасность, направленность (профиль) «Информационная безопасность киберфизических систем» и рекомендуется для оценивания уровня сформированности компетенций при проведении текущего контроля успеваемости и промежуточной аттестации студентов по дисциплине «Технологии доверенного взаимодействия киберфизических систем».

5.Срок действия ФОС: на срок реализации образовательной программы.

1. Описание критериев оценивания компетенции на различных этапах их формирования, описание шкал оценивания

Компетенция (ии), индикатор (ы)	Уровни сформированности компетенции(й),			
	Минимальный уровень не достигнут (неудовлетворительно) 2 балла	Минимальный уровень (удовлетворительно) 3 балла	Средний уровень (хорошо) 4 балла	Высокий уровень (отлично) 5 баллов
Компетенция: ПК-1 Способен проводить исследования и анализ информационных процессов защиты информации в киберфизических системах				
ПК-1 ИД-1 технологии поиска, изучения, обобщения, классификации и систематизации научной информации, методы анализа и обоснования выбора решений по обеспечению требуемого уровня безопасности информационных процессов защиты информации в киберфизических системах	на низком уровне: применяет технологии поиска, изучения, обобщения, классификации и систематизации научной информации, методы анализа и обоснования выбора решений по обеспечению требуемого уровня безопасности информационных процессов защиты информации в киберфизических системах	в основном: применяет технологии поиска, изучения, обобщения, классификации и систематизации научной информации, методы анализа и обоснования выбора решений по обеспечению требуемого уровня безопасности информационных процессов защиты информации в киберфизических системах	умеет: применять технологии поиска, изучения, обобщения, классификации и систематизации научной информации, методы анализа и обоснования выбора решений по обеспечению требуемого уровня безопасности информационных процессов защиты информации в киберфизических системах	на высоком профессиональном уровне: применяет технологии поиска, изучения, обобщения, классификации и систематизации научной информации, методы анализа и обоснования выбора решений по обеспечению требуемого уровня безопасности информационных процессов защиты информации в киберфизических системах
ПК-1 ИД-2 применение современных информационных технологий и программных средств, при решении задач профессиональной деятельности	на низком уровне: навыками применения современных информационных технологий и программных средств, в том числе отечественного производства, при решении задач профессиональной деятельности	в основном: навыками применения современных информационных технологий и программных средств, в том числе отечественного производства, при решении задач	владеет: навыками применения современных информационных технологий и программных средств, в том числе отечественного производства, при решении задач профессиональной деятельности	на высоком профессиональном уровне: навыками применения современных информационных технологий и программных средств, в том числе отечественного производства, при решении задач

		профессиональной деятельности		профессиональной деятельности
ПК-1 ИД-4 применяет технологии исследования и анализа информационных процессов защиты информации в киберфизических системах	на низком уровне: применяет технологии исследования и анализа информационных процессов защиты информации в киберфизических системах	в основном: применяет технологии исследования и анализа информационных процессов защиты информации в киберфизических системах	владеет: навыками применения технологий исследования и анализа информационных процессов защиты информации в киберфизических системах	на высоком профессиональном уровне: применяет технологии исследования и анализа информационных процессов защиты информации в киберфизических системах

Оценивание уровня сформированности компетенции по дисциплине осуществляется на основе «Положения о проведении текущего контроля успеваемости и промежуточной аттестации обучающихся по образовательным программам высшего образования - программам бакалавриата, программам специалитета, программам магистратуры - в федеральном государственном автономном образовательном учреждении высшего образования «Северо-Кавказский федеральный университет» в актуальной редакции.

ОЦЕНОЧНЫЕ СРЕДСТВА ДЛЯ ПРОВЕРКИ УРОВНЯ СФОРМИРОВАННОСТИ КОМПЕТЕНЦИЙ

Номер задания	Правильный ответ	Содержание вопроса	Компетенция
		Форма обучения очная, семестр 1	
1.	b	Какое из перечисленных свойств является ключевой характеристикой мультиагентных систем, обеспечивающей способность системы находить решения сложных задач без централизованного управления? a) Модульность b) **Эмерджентность (возникновение коллективного интеллекта из самоорганизации агентов)** c) Гетерогенность d) Детерминированность	ПК-1
2.	a	Какой тип архитектуры взаимодействия агентов предполагает наличие единого управляющего элемента, который координирует действия всей группы? a) **Централизованная архитектура** b) Децентрализованная архитектура c) Распределённая архитектура d) Иерархическая архитектура с горизонтальными связями	ПК-1
3.	a	Что из перечисленного является обязательным требованием к функционированию мультиагентной системы? a) **Включение в систему агентов, выполняющих различные функции и взаимодействующих между собой для достижения общей цели** b) Наличие единого жёстко заданного алгоритма для всех агентов c) Полная автономность каждого агента без обмена информацией d) Отсутствие возможности динамического изменения состава системы	ПК-1
4.	a	Какое фундаментальное различие между мультиагентной системой и традиционной распределённой системой обработки данных? a) **В МРТС агенты обладают** квази-субъектностью**, т.е. способностью к автономному целенаправленному поведению** b) В МРТС все агенты идентичны по своей функциональности	ПК-1

		c) В МРТС отсутствуют коммуникационные протоколы d) В МРТС каждый агент имеет доступ ко всей информации системы	
5.	b	Что является основным объектом исследования при анализе информационных процессов защиты в МРТС? a) Отдельный робот-агент b) **Информационное взаимодействие между агентами, сенсорами и средой** c) Только шифрование каналов связи d) Исключительно физическая защита роботов	ПК-1
6.	b	Какое ключевое преимущество даёт мультиагентный, распределённый подход к созданию искусственного интеллекта автономных систем? a) Упрощение разработки программного обеспечения b) **Возможность решения широкого комплекса задач в сферах охраны среды, медицины, патрулирования за счёт коллективных действий** c) Снижение требований к вычислительным ресурсам каждого агента d) Исключение необходимости в системах связи между агентами	ПК-1
7.	b	Какая из архитектур управления МРТС является наиболее уязвимой к атакам типа «отказ в обслуживании» на центральный узел? a) Децентрализованная b) **Централизованная** c) Полностью распределённая (одноранговая) d) Гибридная с резервным копированием	ПК-1
8.	a	Какое свойство МРТС напрямую усложняет задачи информационной безопасности из-за разнородности состава агентов (разные ОС, протоколы, производители)? a) **Гетерогенность (неоднородность)** b) Масштабируемость c) Адаптивность d) Автономность	ПК-1
9.	a	В чем заключается принципиальное отличие «роевой» (swarm) робототехнической системы от классической мультиагентной? a) **В роевых системах агенты обычно однородны, взаимодействуют по локальным правилам, а коллективный интеллект возникает снизу вверх без явного разделения ролей**	ПК-1

		b) В роевых системах обязательно присутствует центральный координатор c) Роевые системы не используют беспроводную связь d) В роевых системах каждый агент выполняет строго уникальную функцию	
10.	a	Какое ключевое свойство мультиагентных систем порождает динамическую нестационарность среды с точки зрения анализа безопасности? a) **Способность системы к самоорганизации и адаптации в реальном времени** b) Статичность состава агентов c) Предопределённость всех сценариев взаимодействия d) Отсутствие обратных связей между агентами	ПК-1
11.	a	Какая из перечисленных архитектур взаимодействия агентов в наибольшей степени соответствует парадигме «отсутствия единой точки отказа»? a) **Полностью децентрализованная (одноранговая) сеть** b) Клиент-серверная архитектура c) Архитектура с выделенным координатором d) Иерархическая архитектура с одним главным узлом	ПК-1
12.	a	Какое свойство МРТС, связанное с открытостью, создаёт наибольшие риски для информационной безопасности? a) **Открытость системы для подключения новых агентов без жёсткой предварительной авторизации** b) Закрытость протоколов взаимодействия c) Отсутствие внешних интерфейсов d) Полная изоляция от других информационных систем	ПК-1
13.	b	Согласно систематическому обзору (Yan et al., 2025), на какие три критические уровня классифицируются угрозы безопасности в робототехнических системах? a) Сенсорный, исполнительный, управляющий b) **Физический, коммуникационный, прикладной** c) Аппаратный, программный, сетевой d) Внутренний, внешний, смешанный	ПК-1
14.	a	Какой тип угроз относится к категории «мягких атак» на мультиагентные робототехнические системы? a) **Перехват сообщений, формирование и передача членам роя дезинформации**	ПК-1

		b) Физическое уничтожение роботов c) Отключение электропитания базовой станции d) Засветка оптических датчиков мощным лазером	
15.	a	В модели нарушителя для МРТС, построенной по аналогии с «полицейским участком», какие два параметра используются для классификации нарушителя? a) **Уровень доступа нарушителя к системе и период его воздействия на систему (основанный на модели жизненного цикла)** b) Тип используемого вредоносного ПО и объём украденных данных c) Географическое расположение нарушителя и его финансирование d) Количество скомпрометированных агентов и скорость распространения атаки	ПК-1
16.	b	Какая специфическая угроза возникает при использовании крупных языковых моделей (LLM) для управления агентами в МРТС? a) Замедление реакции агентов b) **Возможность, при которой злоумышленник через LLM отдаёт вредоносные команды, используя визуальные или аудиоатаки** c) Увеличение энергопотребления d) Усложнение интерфейса программирования	ПК-1
17.	b	Какая угроза характерна именно для мультиагентных систем, но не для одиночных роботов? a) Выход из строя аккумулятора b) **Атака «византийских» узлов, при которой один или несколько скомпрометированных агентов распространяют ложную информацию среди других, нарушая консенсус** c) Отказ сенсора измерения расстояния d) Сбой в работе операционной системы ROS	ПК-1
18.	b	Какой тип атаки относится к «физическому слою» в классификации угроз Yan et al. (2025) для роевых робототехнических систем? a) Подмена сетевых пакетов b) **Физический захват (захват) робота-агента злоумышленником с последующим анализом его памяти и ключей** c) SQL-инъекция в базу данных миссии d) ARP-spoofing в локальной сети	ПК-1

19.	a	Какая угроза безопасности относится к категории «внутренних» по отношению к мультиагентной системе? a) **Компрометация легитимного агента с последующим использованием его для атак на других членов роя («робот-предатель»)** b) Взлом сервера управления из внешней сети c) Перехват радиосигнала между агентами d) DDOS-атака на канал связи со спутника	ПК-1
20.	a	В чем заключается опасность атаки с координированной стратегией поведения вредоносных роботов на рой? a)**Даже при концентрации вредоносных элементов до 51% известные методы не всегда эффективны; атака может привести к принятию группой роботов ошибочного консенсусного решения** b) Атака приводит к немедленному физическому разрушению всех роботов c) Атака требует квантового компьютера для реализации d) Атака воздействует только на одного робота	ПК-1
21.	a	Какое из перечисленных является специфической угрозой информационной безопасности именно для мультиагентной робототехнической системы (в отличие от обычной компьютерной сети)? a) **Распространение ложных данных о цели группировки и использование искажённой информации** b) Кража паролей пользователей c) Отказ в обслуживании веб-сервера d) Фишинговая атака на оператора	ПК-1
22.	a	Какая уязвимость в операционной системе ROS (Robot Operating System) представляет собой критическую угрозу при построении мультиагентной системы? **a) Отсутствие встроенных механизмов шифрования и аутентификации для сообщений между узлами по умолчанию** b) Сложность установки и настройки c) Низкая производительность при большом количестве узлов d) Отсутствие поддержки реального времени	ПК-1
23.	a	Что такое атака «51 процент» применительно к роевым робототехническим системам?	ПК-1

		a) **Ситуация, когда концентрация вредоносных роботов в рое превышает половину (более 50%), позволяя им навязывать ложный консенсус остальным** b) Атака на 51-й порт сервера управления c) Вывод из строя 51% батарей всех роботов d) Кибератака, длящаяся 51 минуту	
24.	d	Согласно многочисленным исследованиям, какой уровень концентрации вредоносных элементов в рое является критическим порогом, после которого стандартные методы защиты становятся неэффективными? a) 10% b) 25% c) 45% d) **51%**	ПК-1
25.	a	Что предлагается использовать в доверительной модели информационной безопасности среды многоагентных систем для повышения безопасности в неконтролируемой среде? a) **Оценку доверия к среде эксплуатации как части информационного взаимодействия, включая локализацию внешнего нарушителя** b) Полный запрет на любую коммуникацию между агентами c) Использование только проводных каналов связи d) Периодическое отключение всех агентов от питания	ПК-1
26.	a	Какой метод обеспечения безопасности в МРТС основан на квантификации процесса достижения консенсуса членами группы с последующей обработкой информации? a) **Алгоритм защиты от координированных атак вредоносных роботов, использующий внутри- и межпериодный анализ для выявления аномалий** b) Метод полного перебора всех возможных состояний системы c) Алгоритм случайной маршрутизации сообщений d) Метод одноразовых паролей для каждого агента	ПК-1
27.	c	Какое из перечисленных направлений НЕ относится к основным методам обеспечения безопасности мультиагентных систем согласно обзорной статье Wang et al. (2025)? a) Шифрование и аутентификация	ПК-1

		b) Обнаружение вторжений и реагирование c) **Использование исключительно симметричных ключей без их ротации** d) Управление репутацией и проектирование отказоустойчивости	
28.	a	Какая технология распределённого реестра может использоваться для повышения доверия и отслеживания репутации агентов в децентрализованной МРТС? a) **Блокчейн (или DLT) для создания неизменяемого журнала взаимодействий и оценок репутации агентов** b) Централизованная SQL-база данных c) Файловая система NFS d) Электронные таблицы Excel	ПК-1
29.	a	Каким образом может быть расширен метод безопасности на основе доверия и репутации для МРТС? a) **Путём учёта среды эксплуатации системы как части информационного взаимодействия** b) Путём отказа от любых метрик доверия c) Путём ручного назначения рейтинга каждому агенту d) Путём игнорирования истории взаимодействий	ПК-1
30.	a	В алгоритме защиты роевых систем от атак вредоносных роботов, что является ключевой метрикой для выявления аномалий? a) **Отклонение поведения конкретного робота от консенсусного решения группы в последовательные периоды** b) Уровень заряда батареи робота c) Скорость перемещения робота d) Цвет корпуса робота	ПК-1
31.	a	Какой метод обнаружения вторжений особенно актуален для МРТС с децентрализованным управлением? a) **Распределённые системы обнаружения вторжений (Distributed IDS), где агенты наблюдают за поведением своих соседей** b) Централизованный IDS на единственном сервере c) Отсутствие IDS как принцип d) IDS только на физическом уровне	ПК-1

32.	a	Какое преимущество даёт использование моделей доверия и репутации в МРТС? a) **Повышение эффективности и защищённости системы за счёт учёта истории взаимодействий и отказа от взаимодействия с ненадёжными агентами** b) Полное исключение возможности компрометации агентов c) Упрощение архитектуры системы до одного узла d) Снижение требований к вычислительным ресурсам	ПК-1
33.	a	Какое направление развития методов безопасности МРТС связано с использованием гомоморфного шифрования? a) **Возможность выполнения операций над зашифрованными данными (например, агрегация сенсорных показаний) без их расшифровки, что сохраняет конфиденциальность даже при компрометации узла агрегации** b) Увеличение скорости шифрования данных c) Упрощение процесса обмена ключами d) Отказ от шифрования в пользу контрольных сумм	ПК-1
34.	a	Какая архитектура безопасности предлагается для многоагентных семантических коммуникационных сетей (SemComNet)? a) **Трёхуровневая архитектура: уровень управления, семантической передачи и когнитивного восприятия** b) Двухуровневая архитектура «клиент-сервер» c) Одноуровневая архитектура «общая шина» d) Архитектура «звезда» с одним центральным агентом	ПК-1
35.	a	Какая архитектура безопасности предлагается для многоагентных семантических коммуникационных сетей (SemComNet)? a) **Трёхуровневая архитектура: уровень управления, семантической передачи и когнитивного восприятия** b) Двухуровневая архитектура «клиент-сервер» c) Одноуровневая архитектура «общая шина» d) Архитектура «звезда» с одним центральным агентом	ПК-1
36.	a	Какой подход может быть использован для защиты от атак типа «византийские узлы» в МРТС? a) **Использование алгоритмов византийской отказоустойчивости (Byzantine Fault Tolerance, BFT) для достижения консенсуса даже при наличии**	ПК-1

		скомпрометированных агентов b) Периодическая перезагрузка всех агентов c) Отказ от любой координации между агентами d) Использование одного «суперагента», которому все доверяют	
37.	a	В чем заключается специфика применения методов машинного обучения для обеспечения безопасности МРТС? a) **Необходимость в распределённых (федеративных) алгоритмах обучения, которые не требуют сбора всех данных в едином центре из-за ограничений по связи и конфиденциальности** b) Возможность использовать стандартные централизованные датасеты c) Отсутствие потребности в вычислительных ресурсах на агентах d) Машинное обучение не применимо для задач безопасности МРТС	ПК-1
38.	a	Какая метрика используется в доверительных моделях для оценки надёжности среды функционирования МРТС? a) **Вероятность обнаружения субъекта внешнего нарушителя в среде на основе анализа сенсорных данных и истории перемещений** b) Температура окружающего воздуха c) Уровень шума в канале связи d) Количество агентов в системе	ПК-1
39.	c	Какой стандарт считается основополагающим для кибербезопасности промышленных роботов и систем автоматизации, на который ссылаются отраслевые стандарты (например, ISO 10218)? a) ISO 13849 b) IEC 61508 c) **IEC 62443** d) ISO 12100	ПК-1
40.	a	Что нового в области кибербезопасности было введено в версии стандарта ISO 10218 (2025 г.) для промышленных роботов? a) **Обязательное проведение оценки кибербезопасности (cybersecurity risk assessment) на этапе проектирования и интеграции, а также прямая ссылка на IEC 62443** b) Полное исключение требований к кибербезопасности	ПК-1

		c) Требование использовать только проводные соединения d) Запрет на использование любых форм аутентификации	
41.	a	Какие требования безопасности объединяет в себе новая версия стандарта ISO 10218 (2025) для коллаборативных роботов? a) **Безопасность, кибербезопасность и рекомендации по совместной работе (safety, cybersecurity, collaboration guidance)** b) Только механическую безопасность c) Только электромагнитную совместимость d) Только эргономику рабочего места	ПК-1
42.	a	Какой стандарт функциональной безопасности является базовым для многих отраслевых стандартов в робототехнике (включая IEC 62061, ISO 13849)? a) **IEC 61508** b) ISO 9001 c) IEEE 802.11 d) RFC 791	ПК-1
43.	a	Согласно рекомендациям современных методологий, с какими типами систем следует проводить аналогию при анализе угроз безопасности для многоагентных робототехнических систем? a) **С киберфизическими системами (КФС) и интернетом вещей (IoT)** b) С исключительно автономными автомобилями c) С чисто механическими системами без электроники d) С настольными персональными компьютерами	ПК-1
44.	b	Какая новая серия стандартов ISO (находится в стадии разработки) направлена на обеспечение совместимости, безопасности, защищённости и надёжности при взаимодействии нескольких роботов с инфраструктурой? a) ISO 10218 b) **ISO/AWI 26159 (серия стандартов для системных интеграторов)** c) ISO 13849 d) ISO 3691-4	ПК-1
45.	a	Какие основные свойства многоагентных систем должны учитываться при построении их моделей угроз согласно методологии анализа? a) **Открытость, гетерогенность, автономность, кооперативность, динамическая адаптивность и эмерджентность**	ПК-1

		b) Только производительность и надёжность c) Только стоимость и габариты d) Только цвет и форма корпуса	
46.	b	Какой стандарт IEC специально посвящён кибербезопасности и включает профили для различных систем, включая возможность создания «профиля робота»? a) IEC 61508 b) **IEC 62443-1-5** c) IEC 61800-5-2 d) IEC 60204	ПК-1
47.	a	В чём заключается специфика методологии оценки рисков для МРТС по сравнению с традиционными IT-системами? a) **Необходимость учитывать не только киберугрозы, но и физические последствия их реализации (повреждение среды, травмирование людей), а также влияние на динамику коллективного поведения** b) Оценка рисков для МРТС проще, чем для IT-систем c) Физические последствия для МРТС не рассматриваются d) Достаточно только анализа сетевого трафика	ПК-1
48.	a	Какая методология построения политик безопасности рекомендуется для МРТС, действующих в неконтролируемой среде с возможным присутствием злоумышленников? a) **Проактивная методология с непрерывным мониторингом поведения агентов и адаптацией политик на основе моделей доверия** b) Статическая методология «запрещено всё, что не разрешено явно» c) Методология «полного доверия» всем агентам внутри периметра d) Отказ от формальных политик безопасности	ПК-1
49.	a	Какое требование к обновлениям прошивок (firmware) в МРТС диктуется современными стандартами кибербезопасности? a) **Наличие цифровой подписи пакета обновления и возможность его безопасной (аутентифицированной и целостной) доставки** b) Свободное распространение обновлений через открытые форумы c) Обновления только через физический доступ к каждому роботу d) Отсутствие какой-либо проверки подлинности обновлений	ПК-1

50.	a	Что является ключевым элементом методологии «Security by Design» применительно к разработке мультиагентных робототехнических систем? a) **Внедрение механизмов безопасности на самых ранних этапах проектирования архитектуры, а не добавление их «сверху» после создания системы** b) Разработка системы без учёта безопасности с последующей установкой «заплаток» c) Безопасность, обеспечиваемая исключительно физической изоляцией d) Перекладывание ответственности за безопасность на конечного пользователя	ПК-1

2. Описание шкалы оценивания

В рамках рейтинговой системы успеваемость студентов по каждой дисциплине оценивается в ходе текущего контроля и промежуточной аттестации. Рейтинговая система оценки знаний студентов основана на использовании совокупности контрольных мероприятий по проверке пройденного материала, оптимально расположенных на всем временном интервале изучения дисциплины. Принципы рейтинговой системы оценки знаний студентов основываются на требованиях, описанных в Положении об организации образовательного процесса на основе рейтинговой системы оценки знаний студентов в ФГАОУ ВО «СКФУ».

3. Критерии оценивания компетенций*

Оценка «отлично» выставляется студенту, если
- дополняет свой ответ информацией из дополнительных источников;
- в своей речи использует в полном объеме специальные термины;
- ответ логичен и последователен;
- выводы аргументированы и доказательны.

Оценка «хорошо» выставляется студенту, если
- демонстрирует хорошее владение учебной информацией, определенной рамками учебной дисциплины;
- демонстрирует достаточные знания, владеет специальной терминологией;
- ответ на поставленный вопрос излагается систематизировано и последовательно, при этом допускает определенные неточности в подаче материала.

Оценка «удовлетворительно» выставляется студенту, если
- в процессе ответа на вопрос допускает нарушение в последовательности изложения материала;
- неточно употребляет специальные термины;
- не делает выводы по изложенному материалу (поверхностный характер ответа).

Оценка «неудовлетворительно» выставляется студенту, если
- отвечая на вопросы не последователен, не логичен;
- не демонстрирует определенные системы знаний по предмету;
- не владеет основной и дополнительной литературой, не делает выводы;
- не владеет понятийным аппаратом по данной дисциплине.

** в соответствии с результатами освоения дисциплины*