Документ подписан простой электронной подписью
Информация о владельце:
ФИО: Гриб Владислав Валерьевич
Должность: Ректор
Дата подписания: 21.10.2026 17:15:36
Уникальный программный ключ:
637517d24e103c3db032acf37e...

Образовательное частное учреждение высшего образования

«МОСКОВСКИЙ УНИВЕРСИТЕТ ИМЕНИ А.С. ГРИБОЕДОВА»

(ИМПЭ им. А.С. Грибоедова)

МЕЖДУНАРОДНЫЙ ИНСТИТУТ ИННОВАЦИОННОЙ ЭКОНОМИКИ, ЛИДЕРСТВА И МЕНЕДЖМЕНТА

УТВЕРЖДАЮ
Директор Международного института инновационной экономики, лидерства и менеджмента
_____ А. А. Панарин
«17» декабря 2025г.

ФОНД ОЦЕНОЧНЫХ СРЕДСТВ

по учебной дисциплине:

ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ В ЭКОНОМИЧЕСКИХ СИСТЕМАХ

Направление подготовки 38.03.01 Экономика
(уровень бакалавриат)

Направленность (профиль):
« Финансовая разведка и экономическая безопасность»

Форма обучения: очная

Москва

Фонд оценочных средств для дисциплины «Информационная безопасность в экономических системах». Направление подготовки/специальность 38.03.01 Экономика, направленность (профиль/специализация): «Информационная безопасность в экономических системах», Т.В. Новикова – М.: ИМПЭ им. А.С. Грибоедова

Фонд оценочных средств является неотъемлемой частью рабочей программы дисциплины.

Разработчик: Т.В. Новикова

Заведующий кафедрой: / Т. В. Новикова

1. ФОНД ОЦЕНОЧНЫХ СРЕДСТВ ДЛЯ ТЕКУЩЕГО КОНТРОЛЯ УСПЕВАЕМОСТИ, ПРОМЕЖУТОЧНОЙ АТТЕСТАЦИИ ОБУЧАЮЩИХСЯ ПО ДИСЦИПЛИНЕ

Настоящий Фонд оценочных средств (ФОС) по дисциплине «Информационная безопасность в экономических системах» является неотъемлемым приложением к рабочей программе дисциплины (РПД) «Информационная безопасность в экономических системах». На данный ФОС распространяются все реквизиты утверждения, представленные в РПД по данной дисциплине.

2. ПЕРЕЧЕНЬ ОЦЕНОЧНЫХ СРЕДСТВ

Для определения качества освоения обучающимися учебного материала по дисциплине используются следующие оценочные средства:

№ п/п	Оценочное средство	Краткая характеристика оценочного средства	Представление оценочного средства в ФОС
1	Тестирование	Вид контроля, позволяющий оценить изученный теоретический материал.	Вопросы для проведения тестирования
2	Практические задания	Вид контроля, позволяющий оценить умение обучающегося применять осваиваемую компетенцию в практических ситуациях и при решении производственных задач	Задания к практическому занятию
3	Контрольная работа	Вид контроля, позволяющий определить результат освоения компетенций по дисциплине в рамках рассматриваемой темы, оцениваемый с помощью соответствующих индикаторов достижения компетенций	Задания контрольной работы
4	Самостоятельная работа	Вид контроля, позволяющий оценить проработку теоретического материала, изучение рекомендуемой литературы, выполнение практико-ориентированных заданий (заполнение таблиц, проведение сравнительного анализа, составление схем и др.), решение практических задач, создание презентаций, написание рефератов, подборку нормативного и иного материала и выполнение других заданий	Задания самостоятельной работы
5	Курсовая работа	Вид контроля, позволяющий выявить степень владения базовыми знаниями, умениями и навыками, необходимыми для обучения, и определить уровень владения новым материалом	Индивидуальные задания (темы) для курсовой работы
6	Зачет/Зачет с оценкой/Экзамен	Вид контроля, позволяющий выявить степень овладения знаниями, умениями и навыками, необходимыми для дальнейшего освоения образовательной программы подготовки	Вопросы для подготовки к зачету/зачету с оценкой/экзамену

3. ПАСПОРТ ФОНДА ОЦЕНОЧНЫХ СРЕДСТВ ДИСЦИПЛИНЕ

3.1. Сопроводительная информация.

Разработчик	Т.В. Новикова
Кафедра	Финансов, экономики и организации производства
Наименование дисциплины	Информационная безопасность в экономических системах
Факультет / институт	Международный институт инновационной экономики, лидерства и менеджмента
Направление подготовки / специальность	38.03.01 Экономика
Количество вопросов в оценочных заданиях (диапазон)	25
Общее время тестирования (мин)	90
Общее количество вопросов/заданий в ФОС	*42*
Размещенность на сайте Университета примерного перечня вопросов, заданий ФОС – для подготовки обучающихся к прохождению оценки (да / нет)	*Да*

2.2. Характеристика оцениваемых компетенций.

Код компетенции	**Формулировка компетенции**	**Индикаторы достижения компетенции** (для планирования результатов обучения по элементам образовательной программы и соответствующих оценочных средств)
УК-11	Способен формировать нетерпимое отношение к проявлениям экстремизма, терроризма, коррупционному поведению и противодействовать им в профессиональной деятельности	**ИУК-11.1. Знает** методы и принципы формирования нетерпимого отношения к проявлениям экстремизма, терроризма и коррупционному поведению **ИУК-11.2. Умеет** формировать нетерпимое отношение к проявлениям экстремизма, терроризма и коррупционному поведению **ИУК-11.3. Владеет** методами применения правовых норм к проявлениям экстремизма, терроризма и коррупционному поведению

4. СОДЕРЖАНИЕ ОЦЕНОЧНЫХ СРЕДСТВ ТЕКУЩЕГО КОНТРОЛЯ

4.1. ТИПОВЫЕ ТЕСТОВЫЕ ЗАДАНИЯ.

Тесты содержат набор вопросов, в полном объеме охватывающие изученный теоретический материал по указанной теме (индикаторы ЗНАТЬ). Выполнение тестов позволяет определить результат освоения компетенций по дисциплине в рамках рассматриваемой темы, оцениваемый с помощью соответствующих индикаторов достижения компетенций. Индивидуальный тестовый сеанс для каждого обучающегося формируется по специальному алгоритму, обеспечивающему заданную тематическую структуру и пропорциональное наличие вопросов разного типа и сложности.

Примерные тестовые задания

Типовые тестовые задания

Тестовые задания предназначены для проверки знаний обучающихся по темам дисциплины. Каждое задание предполагает выбор одного или нескольких правильных ответов.

1. Что понимается под информационной безопасностью?

а) состояние защищенности информации от несанкционированного доступа, уничтожения, модифицирования, блокирования, копирования, предоставления, распространения

б) совокупность мер по защите компьютерных сетей

в) защита информации от компьютерных вирусов

г) шифрование передаваемых данных

Ответ: а

2. Какие основные составляющие информационной безопасности выделяют?

а) доступность, целостность, конфиденциальность

б) скорость, надежность, стоимость

в) открытость, публичность, доступность

г) шифрование, аутентификация, авторизация

Ответ: а

3. Что такое угроза информационной безопасности?

а) совокупность условий и факторов, создающих опасность нарушения информационной безопасности

б) компьютерный вирус

в) несанкционированный доступ к информации

г) сбой в работе компьютерной системы

Ответ: а

4. Какой федеральный закон регулирует отношения в сфере информации, информационных технологий и защиты информации?

а) Федеральный закон от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и о защите информации»

б) Федеральный закон от 07.08.2001 № 115-ФЗ

в) Федеральный закон от 28.12.2010 № 390-ФЗ «О безопасности»

г) Гражданский кодекс Российской Федерации

Ответ: а

5. Какой федеральный закон регулирует отношения, связанные с обработкой персональных данных?

а) Федеральный закон от 27.07.2006 № 152-ФЗ «О персональных данных»

б) Федеральный закон от 06.04.2011 № 63-ФЗ «Об электронной подписи»

в) Закон РФ от 21.07.1993 № 5485-1 «О государственной тайне»

г) Федеральный закон от 27.07.2006 № 149-ФЗ

Ответ: а

6. Что такое политика безопасности?

а) совокупность документированных правил, процедур, практических приемов, которыми руководствуется организация в своей деятельности по защите информации

б) закон о защите информации

в) программное обеспечение для защиты информации

г) метод шифрования данных

Ответ: а

7. Что такое идентификация в контексте информационной безопасности?

а) присвоение субъектам и объектам доступа идентификатора и сравнение его с заданным перечнем

б) проверка подлинности предъявленного идентификатора

в) шифрование идентификационных данных

г) создание учетной записи пользователя

Ответ: а

8. Что такое аутентификация?

а) проверка принадлежности субъекту доступа предъявленного им идентификатора и подтверждение его подлинности

б) присвоение субъекту идентификатора

в) разграничение доступа к ресурсам

г) регистрация действий пользователя

Ответ: а

9. Какие виды аутентификации существуют?

а) парольная, биометрическая, на основе сертификатов

б) только парольная

в) только биометрическая

г) только аппаратная

Ответ: а

10. Что такое криптография?

а) наука о методах обеспечения конфиденциальности и аутентичности информации

б) наука о компьютерных вирусах

в) наука о компьютерных сетях

г) наука о базах данных

Ответ: а

11. Какие алгоритмы относятся к симметричным алгоритмам шифрования?

а) DES, ГОСТ 34.12-2015, AES

б) RSA, Эль-Гамаля

в) MD5, SHA-1

г) Kerberos, IPsec

Ответ: а

12. Какой алгоритм относится к асимметричным алгоритмам шифрования?

а) RSA

б) DES

в) AES

г) ГОСТ 34.12-2015

Ответ: а

13. Что такое функция хеширования?

а) функция, преобразующая входные данные произвольной длины в выходную строку фиксированной длины

б) функция шифрования данных

в) функция сжатия данных

г) функция кодирования данных

Ответ: а

14. Что такое электронная цифровая подпись?

а) реквизит электронного документа, полученный в результате криптографического преобразования информации, позволяющий установить отсутствие искажений и подтвердить подлинность документа

б) подпись, выполненная в электронном виде

в) пароль пользователя

г) цифровой сертификат

Ответ: а

15. Что такое межсетевой экран?

а) программное или аппаратное средство, контролирующее и фильтрующее проходящий через него сетевой трафик в соответствии с заданными правилами

б) антивирусная программа

в) программа для шифрования данных

г) сетевая операционная система

Ответ: а

16. Что такое VPN (виртуальная частная сеть)?

а) технология, обеспечивающая защищенное соединение между сетями через открытую сеть (Интернет)

б) локальная компьютерная сеть

в) глобальная сеть

г) беспроводная сеть

Ответ: а

17. Что такое анализ защищенности?

а) процесс выявления уязвимостей в системе защиты информации

б) процесс шифрования данных

в) процесс создания паролей

г) процесс резервного копирования

Ответ: а

18. Что такое компьютерный вирус?

а) программа, способная создавать свои копии и внедряться в другие программы, файлы, загрузочные сектора

б) сбой в работе компьютера

в) ошибка в программном обеспечении

г) вредоносное оборудование

Ответ: а

19. Что такое протоколирование в информационной безопасности?

а) сбор и накопление информации о событиях, происходящих в информационной системе

б) создание протоколов взаимодействия

в) шифрование данных

г) резервное копирование

Ответ: а

20. Что такое аудит в информационной безопасности?

а) анализ накопленной информации о событиях с целью выявления нарушений безопасности

б) проверка бухгалтерской отчетности

в) проверка программного обеспечения

г) тестирование компьютерной сети

Ответ: а

21. Какая модель управления доступом основана на ролях пользователей?

а) ролевая модель управления доступом (RBAC)

б) модель дискреционного доступа

в) модель Белла-ЛаПадулы

г) модель мандатного доступа

Ответ: а

22. Что относится к мерам процедурного уровня информационной безопасности?

а) управление персоналом, физическая защита, поддержка работоспособности, реагирование на нарушения

б) только шифрование данных

в) только установка антивирусов

г) только разработка политики безопасности

Ответ: а

23. Какой стандарт определяет «Общие критерии оценки безопасности информационных технологий»?

а) ГОСТ Р ИСО/МЭК 15408

б) ГОСТ Р ИСО/МЭК 17799

в) ГОСТ Р ИСО/МЭК 27001

г) ГОСТ 34.12-2015

Ответ: а

24. Какой стандарт определяет требования к системе управления безопасностью информации?

а) ГОСТ Р ИСО/МЭК 27001

б) ГОСТ Р ИСО/МЭК 15408

в) ГОСТ 34.12-2015

г) ГОСТ Р 34.10-2012

Ответ: а

25. Что такое социальный инжиниринг?

а) метод несанкционированного доступа к информации, основанный на психологическом воздействии на людей

б) метод шифрования данных

в) метод анализа защищенности

г) метод резервного копирования

Ответ: а

Критерии оценивания тестового задания:

Оценка	Критерии оценивания
отлично	от 90 до 100 % правильно выполненных заданий
хорошо	от 70 до 89 % правильно выполненных заданий
удовлетворительно	от 50 до 69 % правильно выполненных заданий
неудовлетворительно	менее 50 % правильно выполненных заданий

4.2 ТИПОВЫЕ ПРАКТИЧЕСКИЕ ЗАДАНИЯ

Практические задания должны отражать умение обучающегося применять осваиваемую компетенцию в практических ситуациях и при решении производственных задач (индикаторы УМЕТЬ, ВЛАДЕТЬ).

Типовые практические задания (задачи)

Практические задания направлены на оценку сформированности умений (ИУК-11.2) и навыков (ИУК-11.3) обучающихся.

Задание 1. Разработка политики безопасности организации.

Разработайте проект политики информационной безопасности для организации (по варианту). Включите в политику: цели и задачи, область действия, основные принципы, требования к защите информации, ответственность сотрудников.

Задание 2. Анализ рисков информационной безопасности.

Проведите анализ рисков информационной безопасности для организации (по варианту). Определите основные угрозы, уязвимости, оцените вероятность реализации угроз и возможный ущерб. Результаты оформите в виде таблицы рисков.

Задание 3. Анализ российского законодательства в области информационной безопасности.

Проведите обзор российского законодательства в области информационной безопасности. Составьте перечень основных федеральных законов и подзаконных актов, регулирующих защиту информации. Охарактеризуйте сферу действия каждого документа.

Задание 4. Создание и управление учетными записями пользователей.

В операционной системе создайте учетные записи пользователей с различными правами доступа. Настройте параметры парольной политики (минимальная длина пароля, срок действия, сложность). Продемонстрируйте процесс аутентификации пользователей.

Задание 5. Обеспечение безопасности ресурсов с помощью разрешений файловой системы NTFS.

Настройте разрешения файловой системы NTFS для различных пользователей и групп. Установите права на чтение, запись, изменение и полный доступ. Настройте аудит доступа к ресурсам.

Задание 6. Настройка системных параметров безопасности.

Настройте системные параметры безопасности операционной системы: параметры учетных записей, параметры аудита, параметры безопасности сети. Обоснуйте выбранные настройки.

Задание 7. Настройка параметров безопасности подключения к Интернет.

Настройте параметры безопасности подключения к сети Интернет: настройка межсетевого экрана, параметры браузера, настройка антивирусной защиты. Обоснуйте выбранные параметры.

Задание 8. Разработка алгоритмов криптографической защиты.

Разработайте алгоритм шифрования на основе шифра подстановки (по варианту). Зашифруйте заданный текст, продемонстрируйте процесс дешифрования. Оцените криптостойкость разработанного алгоритма.

Задание 9. Анализ защищенности информационной системы.

Проведите анализ защищенности информационной системы с использованием сетевого сканера. Выявите открытые порты, уязвимости. Составьте отчет о результатах анализа и рекомендации по устранению выявленных уязвимостей.

Задание 10. Разработка плана восстановительных работ.

Разработайте план восстановительных работ для организации после нарушения режима информационной безопасности. Включите в план: порядок выявления инцидента, меры по локализации, порядок восстановления работоспособности, анализ причин инцидента.

Критерии оценивания практических занятий:

Оценка	Критерии оценивания
отлично	Выставляется, если обучающийся умеет увязывать теорию с практикой (решает задачи, формулирует выводы, умеет пояснить полученные результаты), владеет понятийным аппаратом, полно и глубоко овладел материалом по заданной теме, обосновывает свои суждения и даёт правильные ответы на вопросы преподавателя
хорошо	Выставляется, если обучающийся умеет увязывать теорию с практикой (решает задачи и формулирует выводы, умеет пояснить полученные результаты), владеет понятийным аппаратом, полно и глубоко овладел материалом по заданной теме, но содержание ответов имеют

	некоторые неточности и требуют уточнения и комментария со стороны преподавателя
удовлетворительно	Выставляется, если обучающийся знает и понимает материал по заданной теме, но изложение неполное, непоследовательное, допускаются неточности в определении понятий, студент не может обосновать свои ответы на уточняющие вопросы преподавателя
неудовлетворительно	Выставляется, если обучающийся допускает ошибки в определении понятий, искажающие их смысл, беспорядочно и неуверенно излагает материал. Делает ошибки в ответах на уточняющие вопросы преподавателя

4.3. ТИПОВЫЕ ЗАДАНИЯ ДЛЯ САМОСТОЯТЕЛЬНОЙ РАБОТЫ

Самостоятельная работа (индикаторы ЗНАТЬ, УМЕТЬ, ВЛАДЕТЬ – на выбор) включает в себя проработку теоретического материала, изучение рекомендуемой литературы, выполнение практико-ориентированных заданий (заполнение таблиц, проведение сравнительного анализа, составление схем и др.), решение практических задач, создание презентаций, написание рефератов, подборка нормативного и иного материала и выполнение других заданий.

Примерные задания для самостоятельной работы

Самостоятельная работа обучающихся направлена на закрепление теоретических знаний, формирование умений и навыков, развитие способности к самостоятельному поиску и анализу информации.

Тема 1. Введение в информационную безопасность

1. Изучите теоретический материал по теме, используя конспект лекций и рекомендуемую литературу.

2. Подготовьте реферат на тему «Информационная безопасность на уровне государства. Концепция безопасности РФ».

3. Подготовьте доклад на тему «Важность проблемы информационной безопасности. Примеры нарушений информационной безопасности».

Тема 2. Законодательный уровень информационной безопасности

1. Изучите Федеральный закон «Об информации, информационных технологиях и о защите информации».

2. Подготовьте обзор международного законодательства в области информационной безопасности.

3. Изучите Федеральный закон «О государственной тайне».

Тема 3. Стандарты и спецификации в области информационной безопасности

1. Изучите руководящие документы Гостехкомиссии России.

2. Подготовьте сравнительную таблицу стандартов информационной безопасности.

3. Изучите содержание ГОСТ Р ИСО/МЭК 15408, 17799, 27001.

Тема 4. Административный уровень информационной безопасности

1. Изучите примеры типовых политик безопасности организации.

2. Разработайте проект политики безопасности для организации (по варианту).

Тема 5. Процедурный уровень информационной безопасности

1. Изучите основные классы мер процедурного уровня.

2. Разработайте план восстановительных работ для организации.

Тема 6. Идентификация и аутентификация

1. Изучите алгоритмы создания одноразовых паролей.

2. Подготовьте доклад на тему «Социальный инжиниринг как угроза информационной безопасности».

Тема 7. Управление доступом. Протоколирование и аудит

1. Изучите системы разграничения доступа.

2. Изучите функциональные компоненты архитектуры систем управления доступом.

Тема 8. Криптографические методы защиты

1. Изучите режимы шифрования блочных шифров.

2. Изучите потоковые шифры.

3. Изучите обмен ключами Диффи-Хелмана.

4. Изучите шифросистему Эль-Гамаля.

5. Изучите стандарт ГОСТ Р 34.10-2012.

Тема 9. Контроль целостности

1. Изучите деятельность удостоверяющих центров.

2. Изучите функцию хеширования MD5.

Тема 10. Экранирование. Тунелирование

1. Изучите технологии VPN IPsec, PPTP.

2. Разработайте конфигурацию межсетевого экрана для организации.

Тема 11. Анализ защищенности

1. Изучите методы антивирусной защиты компьютерной сети.

2. Проведите анализ защищенности информационной системы с использованием сетевого сканера.

Критерии оценивания самостоятельной работы:

Оценка	Критерии оценивания
отлично	выставляется если работа носит научно-исследовательский характер, проанализирован и сделан сравнительный анализ нескольких литературных источников, приведены примеры
хорошо	выставляется если проанализирован и сделан сравнительный анализ нескольких литературных источников, приведены примеры
удовлетворительно	выставляется если проведен сравнительный анализ научно-методической литературы, приведены примеры
неудовлетворительно	выставляется если работа прошла проверку на антиплагиат и соответствует требованиям оформления

5. МАТЕРИАЛЫ ДЛЯ ОЦЕНКИ РЕЗУЛЬТАТОВ ПРОМЕЖУТОЧНОЙ АТТЕСТАЦИИ

Промежуточная аттестация проводится в форме зачета/зачета с оценкой/экзамена.

5.1. Вопросы к зачету/зачету с оценкой/экзамену:

Перечень вопросов

1. Понятие информационной безопасности.

2. Основные составляющие информационной безопасности: доступность, целостность и конфиденциальность.

3. Угрозы информационной безопасности.

4. Задачи системы информационной безопасности.

5. Меры противодействия угрозам безопасности.

6. Основные принципы построения систем защиты АИС.

7. Понятие и важность законодательного уровня информационной безопасности.

8. Обзор российского законодательства в области информационной безопасности.

9. Федеральный закон «Об информации, информационных технологиях и о защите информации».

10. Федеральный закон «Об электронной подписи».

11. Федеральный закон «О персональных данных».

12. Защита авторского права на программные продукты.

13. Оценочные стандарты и технические спецификации.

14. Оценочный стандарт ГОСТ Р ИСО/МЭК 15408 «Общие критерии оценки безопасности информационных технологий».

15. Управленческие стандарты информационной безопасности. ГОСТ Р ИСО/МЭК 17799.

16. ГОСТ Р ИСО/МЭК 27001 «Система управления безопасностью информации. Требования».

17. Административный уровень информационной безопасности: основные понятия.

18. Политика безопасности.

19. Программа безопасности.

20. Синхронизация программы безопасности с жизненным циклом систем.

21. Процедурный уровень информационной безопасности: основные классы мер.

22. Управление персоналом в системе информационной безопасности.

23. Физическая защита.

24. Поддержка работоспособности.

25. Реагирование на нарушение режима безопасности.

26. Планирование восстановительных работ.

27. Понятие идентификации и аутентификации.

28. Парольная аутентификация. Требования к паролям.

29. Одноразовые пароли.

30. Сервер аутентификации Kerberos.

31. Идентификация/аутентификация с помощью биометрических данных.

32. Понятие управления доступом.

33. Модель дискреционного доступа.

34. Модель Белла-ЛаПадулы.

35. Ролевая модель управления доступом.

36. Понятие протоколирования и аудита.

37. Активный аудит.

38. Введение в криптографию. Основные термины и понятия.
39. Типы криптографических систем.
40. Шифры подстановки и перестановки.
41. Блочные шифры. Сеть Фейштеля.
42. Симметричные алгоритмы шифрования: DES, ГОСТ 34.12-2015, AES.
43. Асимметричные алгоритмы шифрования. Алгоритм RSA.
44. Определение функции хеширования. Требования к хеш-функциям.
45. Электронная цифровая подпись. Цифровые сертификаты.
46. Понятие экранирования. Межсетевые экраны.
47. Классификация и виды межсетевых экранов.
48. Понятие тунелирования. Виртуальные частные сети (VPN).
49. Понятие анализа защищенности. Сетевые сканеры.
50. Антивирусная защита. Классификация вирусов.
51. Признаки присутствия на компьютере вредоносных программ.
52. Методы защиты от вредоносных программ. Основы работы антивирусных программ.

Критерии оценивания зачета с оценкой/экзамена:

Оценка	Критерии оценивания
зачтено	Обучающийся должен: уметь строить ответ в соответствии со структурой излагаемого вопроса; продемонстрировать прочное, достаточно полное усвоение знаний программного материала; продемонстрировать знание основных теоретических понятий; правильно формулировать определения; последовательно, грамотно и логически стройно изложить теоретический материал; продемонстрировать умения самостоятельной работы с литературой; уметь сделать достаточно обоснованные выводы по излагаемому материалу.
не зачтено	Обучающийся демонстрирует: незнание значительной части программного материала; не владение понятийным аппаратом дисциплины; существенные ошибки при изложении учебного материала; неумение строить ответ в соответствии со структурой излагаемого вопроса; неумение делать выводы по излагаемому материалу.

Критерии оценивания зачета с оценкой/экзамена:

Оценка	Критерии оценивания
отлично	Выставляется, если обучающимся правильно и полностью раскрыто содержание материала в пределах программы, чётко и правильно даны определения и раскрыто содержание понятий, точно использованы научные и технические термины, в ответе использованы ранее приобретённые теоретические знания, сделаны необходимые выводы и обобщения
хорошо	Выставляется, если обучающимся раскрыто основное содержание материала в пределах программы, даны определения и раскрыто содержание понятий, в ответе использованы ранее приобретённые теоретические знания, сделаны необходимые выводы и обобщения, но присутствуют незначительные нарушения в последовательности изложения, имеются одна-две неточности в содержании ответа

удовлетворительно	Выставляется, если обучающимся содержание учебного материала изложено фрагментарно, не всегда последовательно, не даны определения, не раскрыто содержание понятий, или они изложены с ошибками, допускаются ошибки и неточности в использовании научной терминологии, отсутствуют выводы и обобщения из предыдущего материала, или возможны ошибки в их изложении
неудовлетворительно	Выставляется, если обучающимся основное содержание учебного материала не раскрыто, не даются ответы на основные вопросы, допускаются грубые ошибки в определении понятий, в использовании терминологии, отсутствуют выводы и обобщения