Автономная некоммерческая организация высшего образования «Университет информационных технологий и инноваций»

(АНО ВО УИТИ)

Утверждаю:

Ректор АНО ВО УИТИ Хутинаева С.З.

Сведения об электронной подписи
Подписано: Хутинаева Светлана Зураповна
Должность: ректор
Пользователь: skhutinaeva

Протокол заседания Учёного совета АНО ВО УИТИ № 01 от 26.02.2026 г.

Утверждено на заседании кафедры информатики

Протокол № 01/ ИТ от 24.02.2026 г.

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ
Б1.О.04 МОДУЛЬ ОБЩЕПРОФЕССИОНАЛЬНОЙ ПОДГОТОВКИ
Б1.О.04.13 СРЕДСТВА ЗАЩИТЫ ИНФОРМАЦИИ
Для направления подготовки: 27.03.03 Системный анализ и управление (уровень бакалавриат)
Типы задач профессиональной деятельности: проектно-технологический, научно-исследовательский, эксплуатационно-технологический
Направленность (профиль): Системный анализ и управление бизнес-процессами
Форма обучения: очная

г. Владикавказ, 2026

СОДЕРЖАНИЕ

1. ТРЕБОВАНИЯ К РЕЗУЛЬТАТАМ ОБУЧЕНИЯ ПО ДИСЦИПЛИНЕ (МОДУЛЮ)

Перечень компетенций, формируемых дисциплиной (модулем) в процессе освоения образовательной программы

Код и наименование компетенции	Индикаторы достижения компетенции	Результаты обучения
ОПК-4. Способен осуществлять оценку эффективности технических систем методами системного анализа и управления	ОПК-4.1. Применяет основы системного анализа и методы оценки эффективности технических систем	Знает: показатели надёжности, безопасности и эксплуатационных характеристик технических устройств. Умеет: оценивать состояние и перспективы развития технических систем. Владеет: навыком вычислять технико-экономические показатели для выбора наилучшего варианта технического решения.
	ОПК-4.2. Демонстрирует способность прогнозирования изменений состояния объекта и выработки рекомендации по управлению системой	Знает: современные инструменты моделирования и прогнозирования состояний технических систем. Умеет: моделировать и прогнозировать состояний технических систем. Владеет: навыком прогнозировать изменение состояния объекта и выработать рекомендации по управлению системой.

2. РЕЗУЛЬТАТЫ ОСВОЕНИЯ ДИСЦИПЛИНЫ (МОДУЛЯ)

Цель: Формирование у обучающихся теоретических знаний и практических навыков применения методов и средств защиты информации в профессиональной деятельности.

Задачи:

– Формирование системы знаний в сфере источников угроз безопасности информации в компьютерной системе

– Формирование системы знаний в сфере юридических основ правового обеспечения безопасности компьютерных систем

– Формирование системы знаний о технических и программных средствах обеспечения безопасности компьютерных систем.

3. ОБЪЕМ ДИСЦИПЛИНЫ И РАСПРЕДЕЛЕНИЕ ВИДОВ УЧЕБНОЙ РАБОТЫ ПО СЕМЕСТРАМ

Общая трудоемкость дисциплины «Средства защиты информации» составляет: 5 з.е. / 180 час.

Вид учебной работы								
Аудиторные занятия				**Самостоятельная работа**		**Промежуточная аттестация**		
Аудиторные занятия *в том числе:*	Лекции	Практические занятия	Лабораторные работы	Самостоятельная работа *в том числе:*	часы на выполнение КР / КП	Вид	Семестр	Трудоемкость (час.)
Всего число часов и (или) зачетных единиц (по формам обучения)								
Очная форма обучения								
72	36	36	-	**72**	-	Экзамен	4	**36**
Общая трудоемкость з.е. / час.: 5 з.е. / 180 час.								

4. СОДЕРЖАНИЕ ДИСЦИПЛИНЫ

Тема 1. Введение в информационную безопасность	Лекции ч.	Практические занятия ч.	Лабораторные работы ч.	Самостоят. работа ч.
	4	4	-	14
	Особенности обеспечения информационной безопасности Российской Федерации (роль и место информационной безопасности в общей системе национальной безопасности РФ. Основные цель и задачи обеспечения информационной безопасности РФ. Объекты информационной безопасности РФ. Внешние и внутренние источники угроз информационной безопасности в РФ).			

Тема 2. Организационно-правовое обеспечение защиты информации	Лекции ч.	Прак зан ч.	Лаб раб ч.	Самост раб ч.
	8	8	-	14
	Международные и отечественные стандарты в сфере защиты информации (роль стандартов информационной безопасности. Международные стандарты информационной безопасности. Стандарты для беспроводных сетей. Стандарты информационной безопасности в Интернет. Отечественные стандарты безопасности информационных технологий). Для анализа сетевой безопасности: Security Onion (дистрибутив для мониторинга сетевой безопасности), Nmap (сканер портов). Виртуальные лаборатории: Готовые уязвимые виртуальные машины			

Тема 3. Методы и средства	Лекции ч.	Прак зан ч.	Лаб раб ч.	Самост раб ч.
	8	8	-	14

технической защиты информации	Виды и методы технической защиты информации (пассивные и активные методы защиты информации. Средства технической защиты информации. Защита помещений. Системы охранной сигнализации на территории и в помещениях. Системы видеонаблюдения. Системы контроля доступа. Системы контроля вскрытия аппаратуры).

Тема 4. Программно-технические средства защиты информации	Лекции ч.	Прак зан ч.	Лаб раб ч.	Самост раб ч.
	8	8	-	14
	Защита информации от несанкционированного доступа (идентификация пользователей и установление их подлинности при доступе к компьютерным ресурсам. Идентификация и аутентификация субъектов “пользователь” и “процесс” при запросах на доступ к компьютерным ресурсам. Использование простого и динамически изменяющегося паролей. Биометрическая идентификация. Предотвращение несанкционированного доступа к компьютерным ресурсам и защита программных средств. Разграничение доступа. Защита программных средств от несанкционированного копирования и модификации.			

Тема 5. Криптографические средства защиты информации	Лекции ч.	Прак зан ч.	Лаб раб ч.	Самост раб ч.
	8	8	-	16
	Принципы криптографической защиты информации (основные понятия криптографической защиты информации. Симметричные криптосистемы шифрования. Асимметричные криптосистемы шифрования. Комбинированные криптосистемы шифрования. Электронная цифровая подпись и функция хэширования. Правовые аспекты применения электронной цифровой подписи.			

5. ФОНД ОЦЕНОЧНЫХ СРЕДСТВ ПО ДИСЦИПЛИНЕ

Примерный фонд оценочных средств представлен в Приложении 1.

6. УЧЕБНО-МЕТОДИЧЕСКОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ

Рекомендуемая литература

1 Шаньгин, В. Ф. Информационная безопасность и защита информации / В. Ф. Шаньгин. — 3-е изд. — Саратов: Профобразование, 2024. — 702 с. — ISBN 978-5-4488-0070-2. — Текст: электронный // Цифровой образовательный ресурс IPR SMART: [сайт]. — URL: https://www.iprbookshop.ru/145912.html

2 Прокопенко, Е. В. Техническая защита информации: учебное пособие / Е. В. Прокопенко, В. О. Коротин. — Кемерово: Кузбасский государственный технический университет имени Т.Ф. Горбачева, 2024. — 131 с. — ISBN 978-5-00137-494-7. — Текст:

электронный // Цифровой образовательный ресурс IPR SMART: [сайт]. — URL: https://www.iprbookshop.ru/148668.html

3 Штеренберг, С. И. Защита информации в компьютерных системах: учебное пособие / С. И. Штеренберг. — Санкт-Петербург: Санкт-Петербургский государственный университет промышленных технологий и дизайна, 2022. — 81 с. — ISBN 978-5-7937-2184-4. — Текст: электронный // Цифровой образовательный ресурс IPR SMART: [сайт]. — URL: https://www.iprbookshop.ru/140114.html

4 Программно-аппаратные средства защиты информации: учебное пособие / С. А. Зырянов, М. А. Кувшинов, И. А. Огнев, И. В. Никрошкин. — Новосибирск: Новосибирский государственный технический университет, 2023. — 80 с. — ISBN 978-5-7782-4905-9. — Текст: электронный // Цифровой образовательный ресурс IPR SMART: [сайт]. — URL: https://www.iprbookshop.ru/155427.html

5 Горюнов, В. Е. Организационные основы защиты информации: учебник / В. Е. Горюнов. — Челябинск: Южно-Уральский технологический университет, Челябинский государственный университет, 2025. — 354 с. — ISBN 978-5-6050860-6-2. — Текст: электронный // Цифровой образовательный ресурс IPR SMART: [сайт]. — URL: https://www.iprbookshop.ru/149883.html

7. ИНФОРМАЦИОННО-СПРАВОЧНОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ

7.1 Лицензионное программное обеспечение

- Microsoft Windows 10/11.
- Modelio / StarUML (Средства моделирования систем (UML);
- RStudio / Anaconda (Python) (Среды для системного анализа данных);
- PyCharm Community Edition (Среда разработки (версия Community).

7.2 Свободно распространяемое программное обеспечение:

- Astra Linux Common Edition (отечественное ПО)
- LibreOffice (свободно распространяемое ПО (Open Source)
- Яндекс.Браузер (отечественное ПО)
- 7-Zip
- PostgreSQL/pgAdmin [Система управления базами данных; свободно распространяемое ПО

7.3 Перечень современных профессиональных баз данных, информационных справочных систем и ресурсов сети Интернет:

1. https://ro-edu.ru/ - Медиапортал «Российское образование»
2. http://www.iprbookshop.ru - Электронно-библиотечная система IPRSmart (ЭБС IPRSmart) –электронная библиотека по всем отраслям знаний
3. https://www.elibrary.ru/ - электронно-библиотечная система eLIBRARY.RU, крупнейшая в России электронная библиотека научных публикаций

4. https://cyberleninka.ru/ - научная электронная библиотека КиберЛенинка
5. https://gufo.me/ - справочная база энциклопедий и словарей
6. http://www.consultant.ru/ - справочная правовая система КонсультантПлюс
7. https://www.garant.ru/ - справочная правовая система Гарант
8. https://rosstat.gov.ru/emiss Единая межведомственная информационно-статистическая система (ЕМИСС) Государственная база статистических данных
9. https://minfin.gov.ru/ru/perfomance/audit/standarts/international/documents/?ysclid=mn6p22hks7190904011 - База данных международных стандартов аудита (МСА) [Профессиональный ресурс на сайте IFAC;
10. https://sroaas.ru/auditor/pravila_i_standarty/standarty-audita/ - База данных международных стандартов аудита (МСА) на сайте МФБ (ifac.org) — первоисточники для аудиторской деятельности

8. МАТЕРИАЛЬНО-ТЕХНИЧЕСКОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ

При реализации образовательной программы для освоения учебной дисциплины используются следующие компоненты материально-технической базы Университета:

1. Аудиторный фонд.
2. Материально-технический фонд.
3. Библиотечный фонд.

Аудиторный фонд представляет собой аудитории для проведения учебных занятий, в том числе, лекционных занятий, практических занятий/лабораторных работ.

Материально-технический фонд представлен учебной мебелью и соответствующим оборудованием, обеспечивающим освоение учебной дисциплины.

Библиотечный фонд обеспечивает доступ каждого обучающегося к электронно-библиотечной системе, современным профессиональным базам, информационно-справочным системам, информационным ресурсам сети Интернет, указанным в рабочей программе дисциплины.

Перечень материально-технического обеспечения по дисциплине:

Аудитория для проведения учебных занятий:

Комплект специализированной учебной мебели, отвечающий всем установленным нормам и требованиям: столы, стулья. Персональные компьютеры с программным обеспечением, с возможностью подключения к сети «Интернет». Шкаф книжный, стеллаж, шкаф книжный, стеллаж, доска передвижная поворотная магнитная (маркерная), тумба, доска передвижная магнитная (маркерная).

Рабочее место преподавателя: стол, стул, персональный компьютер с программным обеспечением, с возможностью подключения к сети «Интернет».

Помещение для самостоятельной работы обучающихся:

Комплект специализированной учебной мебели, отвечающий всем установленным нормам и требованиям: столы, стулья.

Персональные компьютеры с программным обеспечением, с возможностью подключения к сети «Интернет».

Аудитория для проведения учебных занятий для обучающихся с ограниченными возможностями здоровья, инвалидов:

Комплект специализированной мебели, отвечающий всем установленным нормам и требованиям для обучающихся с ограниченными возможностями здоровья, инвалидов: столы, стулья, инвалидное кресло-коляска. Гарнитура, информационная система «Исток» - для слабослышащих, клавиатура Брайля, шкаф книжный.

Рабочее место преподавателя: стол, стул, тумба, персональный компьютер с программным обеспечением, с возможностью подключения к сети «Интернет».

9. МЕТОДИЧЕСКИЕ РЕКОМЕНДАЦИИ ДЛЯ ОБУЧАЮЩИХСЯ ПО ОСВОЕНИЮ ДИСЦИПЛИНЫ

Обучение по дисциплине предполагает освоение учебного материала на аудиторных занятиях и в ходе самостоятельной работы. Аудиторные занятия проходят в форме лекций и практических занятий/лабораторных работ.

Для успешного освоения дисциплины рекомендуется придерживаться системного подхода к учебному процессу. Просматривать все лекции, так как они формируют теоретический каркас дисциплины и помогают выстроить логику взаимосвязи ключевых понятий. Рекомендуется вести конспект лекции, с выделением основных идей, вопросов для уточнения и собственных ассоциаций — это поможет в подготовке к активной работе на практических занятиях. На семинарских и практических занятиях целесообразно участвовать в дискуссиях, аргументируя свою позицию и анализируя позиции коллег.

При подготовке к работе во время проведения практических/ лабораторных занятий следует обратить внимание на следующие моменты: на процесс предварительной подготовки, на работу во время занятия, обработку полученных результатов, исправление полученных замечаний.

Предварительная подготовка к практическому/лабораторному занятию заключается в изучении теоретического материала в отведенное для самостоятельной работы время, ознакомление с инструктивными материалами с целью осознания задач практического занятия/лабораторной работы, техники безопасности при работе с оборудованием.

Самостоятельная работа является равноправной частью обучения: целесообразно изучать рекомендованную литературу, дополняя лекционный материал аналитическими источниками и современными исследованиями. Рекомендуется выделять время на систематизацию знаний — составление схем, таблиц, глоссария терминов значительно облегчит подготовку к промежуточной аттестации.

При выполнении самостоятельных заданий целесообразно сфокусироваться на глубине проработки темы и умении применять знания к анализу конкретных ситуаций. Рекомендуется использовать цифровые образовательные ресурсы, современные профессиональные базы, электронные библиотечные системы и информационно-справочные системы для расширения информационной базы.

Рекомендуется регулярно проводить самодиагностику: формулировать ответы на ключевые вопросы без опоры на конспекты, чтобы выявить слабые места. Целесообразно готовиться к занятиям заранее, знакомясь с темой — это позволяет участвовать в учебном процессе на уровне диалога, а не пассивного восприятия.

Успешное освоение дисциплины возможно только при синтезе всех форм работы: лекции задают направление, практические занятия/лабораторные работы развивают

умения и навыки, а самостоятельная работа формирует устойчивые компетенции. Необходимо подходить к обучению как к осознанному проектированию собственного интеллектуального развития, а не как к формальному выполнению требований учебного плана.

Приложение 1

Автономная некоммерческая организация высшего образования «Университет информационных технологий и инноваций»

(АНО ВО УИТИ)

ФОНД ОЦЕНОЧНЫХ СРЕДСТВ
Текущего контроля и промежуточной аттестации по дисциплине (модулю)
Б1.О.04.13 СРЕДСТВА ЗАЩИТЫ ИНФОРМАЦИИ
Для направления подготовки: 27.03.03 Системный анализ и управление (уровень бакалавриат)
Типы задач профессиональной деятельности: проектно-технологический, научно-исследовательский, эксплуатационно-технологический
Направленность (профиль): Системный анализ и управление бизнес-процессами
Форма обучения: очная

г. Владикавказ, 2026

ТИПОВЫЕ КОНТРОЛЬНЫЕ ЗАДАНИЯ ТЕКУЩЕГО КОНТРОЛЯ И ПРОМЕЖУТОЧНОЙ АТТЕСТАЦИИ ПО ДИСЦИПЛИНЕ

Примерные темы для практических занятий

1. Особенности обеспечения информационной безопасности Российской Федерации (роль и место информационной безопасности в общей системе национальной безопасности РФ.
2. Основные цель и задачи обеспечения информационной безопасности РФ. Объекты информационной безопасности РФ. Внешние и внутренние источники угроз информационной безопасности в РФ).
3. Международные и отечественные стандарты в сфере защиты информации (роль стандартов информационной безопасности. Международные стандарты информационной безопасности. Стандарты для беспроводных сетей. Стандарты информационной безопасности в Интернет. Отечественные стандарты безопасности информационных технологий).
4. Для анализа сетевой безопасности: Security Onion (дистрибутив для мониторинга сетевой безопасности), Nmap (сканер портов). Виртуальные лаборатории: Готовые уязвимые виртуальные машины
5. Виды и методы технической защиты информации (пассивные и активные методы защиты информации. Средства технической защиты информации. Защита помещений. Системы охранной сигнализации на территории и в помещениях. Системы видеонаблюдения. Системы контроля доступа. Системы контроля вскрытия аппаратуры).
6. Защита информации от несанкционированного доступа (идентификация пользователей и установление их подлинности при доступе к компьютерным ресурсам. Идентификация и аутентификация субъектов “пользователь” и “процесс” при запросах на доступ к компьютерным ресурсам. Использование простого и динамически изменяющегося паролей.
7. Биометрическая идентификация. Предотвращение несанкционированного доступа к компьютерным ресурсам и защита программных средств. Разграничение доступа. Защита программных средств от несанкционированного копирования и модификации. Для изучения криптографии
8. Принципы криптографической защиты информации (основные понятия криптографической защиты информации. Симметричные криптосистемы шифрования.
9. Асимметричные криптосистемы шифрования. Комбинированные криптосистемы шифрования. Электронная цифровая подпись и функция хэширования.
10. Правовые аспекты применения электронной цифровой подписи). Для изучения криптографии

Примерные темы рефератов

1. Конфиденциальность информации – это известность ее содержания только имеющим соответствующие полномочия субъектам.
2. Методы и средства защиты информации – это организационно-технические и

3. Непреднамеренное воздействие на защищаемую жестком магнитном диске компьютера).

организационно-правовые мероприятия, проводимые в процессе создания и эксплуатации компьютерной системы для обеспечения защиты информации.

4. Политика безопасности — это набор документированных норм, правил и практических приемов, регулирующих управление, защиту и распределение информации ограниченного доступа.

5. Разглашение – это доведение защищаемой информации до неконтролируемого количества получателей информации (например, публикация информации на открытом сайте в сети Интернет или в открытой печати).

6. Собственник информационных ресурсов, систем и технологий – это субъект с полномочиями владения, пользования и распоряжения указанными объектами.

7. Угроза безопасности информации в компьютерной системе – это событие или действие, которое может вызвать изменение функционирования компьютерной системы, связанное с нарушением защищенности, обрабатываемой в ней информации.

8. Утечка – это неконтролируемое распространение защищаемой информации путем ее разглашения, несанкционированного доступа к ней и получения разведками.

9. Уязвимость информации – это возможность возникновения на каком-либо этапе жизненного цикла компьютерной системы такого ее состояния, при котором создаются условия для реализации угроз безопасности информации.

10. Целостность информации – неизменность информации в условиях ее случайного и (или) преднамеренного искажения или разрушения.

Примеры тестовых заданий

1 Упорядоченная совокупность документов и массивов документов и информационных технологий,

реализующих информационные процессы, называется:

a) информационной системой;
b) политикой безопасности;
c) информационной технологией;
d) информационным процессором.

2 Деятельность по предотвращению утечки защищаемой информации, несанкционированных и непреднамеренных воздействий на защищаемую информацию, называется

Защитой информации

3 Получение защищаемой информации заинтересованным субъектом с нарушением правил доступа к ней, называется

Несанкционированным доступом

4 Набор документированных норм, правил и практических приемов, регулирующих управление, защиту и распределение информации ограниченного доступа, называется:

a) защитой информации;
b) политикой безопасности;

c) стратегией защиты информации;

d) правилами поведения.

5 Информация, содержание которой может быть понятно любому субъекту, называется:

a) сказкой;

b) инструкцией хакера;

c) криптосистемой;

d) открытым текстом.

6 Доведение защищаемой информации до неконтролируемого количества получателей информации (например, публикация информации на открытом сайте в сети Интернет или в открытой печати):

a) компьютерным шпионажем;

b) разглашением;

c) вредительством;

d) предательством

7 Субъект с полномочиями владения информационными ресурсами, их пользования и распоряжения, называется

a) сетевым администратором;

b) собственником информационных ресурсов;

c) программистом;

d) пользователем.

8 Неконтролируемое распространение защищаемой информации путем ее разглашения, несанкционированного доступа к ней и получения разведками:

a) расползанием информации;

b) информационным предательством;

c) вредительством;

d) утечкой.

9 Возможность возникновения на каком-либо этапе жизненного цикла компьютерной системы такого ее состояния, при котором создаются условия для реализации угроз безопасности информации, называется:

a) устареванием политики безопасности;

b) сбоем системы защиты информации;

c) уязвимостью информации;

d) обходом защиты информации.

10 Воздействие на защищаемую информацию из-за ошибок пользователя, сбоя технических или программных средств, природных явлений, иных нецеленаправленных воздействий, называется:

a) непреднамеренным воздействием;

b) самоатакой;

c) глюком.

Примерные вопросы для экзамена

1. Какая информация является конфиденциальной?
2. Какие существуют косвенные каналы утечки информации?
3. Какие существуют методы и средства защиты информации?
4. Какие существуют непосредственные каналы утечки информации?
5. Какие существуют уровни правового обеспечения информационной безопасности?
6. Что включают в себя организационные методы защиты информации?
7. Что относится к непреднамеренным угрозам компьютерных систем?
8. Что представляет собой системно-концептуальный подход решении задачи защиты информации в КС?
9. Что такое умышленная угроза информационной безопасности
10. Что является опосредованной угрозой безопасности информации в КС?

Критерии оценивания результатов текущего контроля

1. Оценка прохождения практических занятий производится по шкале «зачтено» / «не зачтено».
2. Оценка подготовки реферата производится по шкале «зачтено» / «не зачтено».
3. Оценка выполнения тестовых заданий формируется следующим образом:

- оценка «отлично» - 85-100% правильных ответов;
- оценка «хорошо» - 70-84% правильных ответов;
- оценка «удовлетворительно» - 40-69% правильных ответов;
- оценка «неудовлетворительно» - менее 39% правильных ответов.

Критерии оценивания результатов при проведении промежуточной аттестации

Знания обучающихся оцениваются по 4-балльной шкале при проведении экзаменов и зачетов с оценкой:

«отлично»,
«хорошо»,
«удовлетворительно»
«неудовлетворительно»)

или 2-балльной шкале при проведении зачета:

«зачтено»,
«не зачтено»

Описание критериев оценивания:

1. *«Отлично» или «зачтено»*

а) Обоснованные объемные ответы на вопросы. Обучающийся иллюстрирует выводы фактами, приводит данные из источников.

б) Обучающийся успешно применяет знание теории для реализации практической части дисциплины. Выполненные задания соответствуют высокому уровню качества, включая использование правильных форматов, методологий и инструментов.

в) Обучающийся умеет анализировать и оценивать нюансы тематики, демонстрируя способность к критическому мышлению и самостоятельному исследованию.

2. *«Хорошо» или «зачтено»*

а) Обучающийся дает достаточно полные ответы на вопросы с учетом основных направлений темы. Ответы обучающегося имеют четкую структуру и логически связаны.

б) Обучающийся применяет теоретические знания в практических заданиях. Выполнение задания в целом соответствует требованиям, допустимы некоторые недочеты или неточные выводы по полученным результатам.

в) Обучающийся демонстрирует хорошее понимание вопроса, знает основные аспекты тематики. Ответы обучающегося содержат достаточно информации, но допустимы недостаточно глубокие суждения.

3. *«Удовлетворительно» или «зачтено»*

а) Ответы на вопросы неполные, не охватывают все стороны тематики и не всегда структурированы или логически связаны. Обучающийся делает верные выводы, но они недостаточно аргументированы или основаны на поверхностном понимании предмета вопроса.

б) Обучающийся способен использовать теоретические знания в практических заданиях, но недостаточно уверен в верности примененных методов и точности в их выполнении. Выполненное задание может содержать некоторые ошибки, недочеты или расхождения.

в) Обучающийся охватывает большинство основных сторон темы вопроса, но демонстрирует неполное или поверхностное их понимание, дает недостаточно развернутые объяснения.

4. *«Неудовлетворительно» или «не зачтено»*

а) Обучающийся отвечает на вопросы неполно, не раскрывает основных направлений темы. Ответы обучающегося не структурированы, не связаны с вопросом, отсутствует логика изложения. Выводы, представляют простые утверждения без анализа или четкой аргументации.

б) Обучающийся не умеет переносить теоретические знания в практическую плоскость и не способен применять их для выполнения задания. Выполненное задание содержит много ошибок, а его результаты не соответствуют поставленным требованиям и (или) неправильно интерпретируются.

в) Ответ обучающегося фрагментарный или отрывочный, не включает анализ рассматриваемого вопроса, пропущены важные детали и связи, поверхностный.