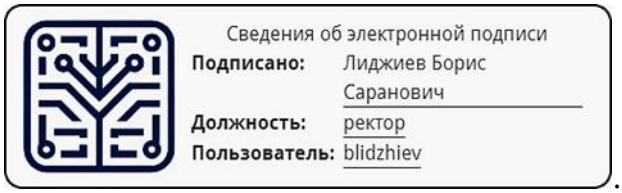
Автономная некоммерческая организация высшего образования
«Информационно-технологический университет»
(АНО ВО ИТУ)

УТВЕРЖДАЮ

Ректор АНО ВО ИТУ Лиджиев Б.С.



Протокол Ученого совета
№3-УС/25-26 от 11.11.2025 г

Утверждено протоколом
заседания кафедры
Математики, информатики и
естественнонаучных дисциплин
№ 3 от 30.10.2025 г.

ДОПОЛНИТЕЛЬНАЯ ПРОФЕССИОНАЛЬНАЯ ПРОГРАММА ПОВЫШЕНИЯ КВАЛИФИКАЦИИ

«ЦИФРОВАЯ БЕЗОПАСНОСТЬ В ПРОФЕССИОНАЛЬНОЙ ДЕЯТЕЛЬНОСТИ»

Приложение № 3.3

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ

«ОСНОВЫ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ»

г. Элиста, 2025

Оглавление

ОСНОВЫ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Компетенции, формируемые в результате освоения дисциплины

ПК-1 Способен проводить согласование документации

1. Цели и задачи дисциплины

Цель дисциплины – обучить принципам обеспечения информационной безопасности государства, подходам к анализу его информационной инфраструктуры и решению задач обеспечения информационной безопасности компьютерных систем и сетей.

Задачи дисциплины:

- обеспечения информационной безопасности государства;
- методологии создания систем защиты информации;
- процессов сбора, передачи и накопления информации;
- оценки защищенности и обеспечения информационной безопасности компьютерных систем.

Место дисциплины в структуре ДПП

Место дисциплины в учебном плане: 3

Осваивается в третью неделю обучения, ч: 36 ч

Заочная форма обучения

Объем дисциплины и распределение видов занятий:

Виды учебных занятий	Всего часов по форме обучения
	заочная
Теоретические занятия	8
Практические занятия	8
Самостоятельная работа	20
Текущая аттестация	зачет
Общая трудоемкость в з.е/ час.	1 з.е./36

2. Планируемые результаты обучения по дисциплине:

знать:

- сущность и понятие информационной безопасности, характеристику ее составляющих;
- место информационной безопасности в системе национальной безопасности страны;
- виды, источники и носители защищаемой информации;
- источники угроз безопасности информации и меры по их предотвращению;
- факторы, воздействующие на информацию при ее обработке в автоматизированных (информационных) системах;
- жизненные циклы информации ограниченного доступа в процессе ее создания, обработки, передачи;
- современные средства и способы обеспечения информационной безопасности;

уметь:

- классифицировать защищаемую информацию по видам тайны и степеням секретности;
- классифицировать основные угрозы безопасности информации;

владеть навыками:

- применения основных правил и документов систем сертификации Российской Федерации.

3. Содержание дисциплины

№	Наименование раздела дисциплины	Содержание раздела
1	Теоретические основы информационной безопасности	Понятие информации и информационной безопасности. Информация, сообщения, информационные процессы как объекты информационной безопасности. Обзор защищаемых объектов и систем. Понятие «угроза информации». Понятие «риска информационной безопасности». Примеры преступлений в сфере информации и информационных технологий. Сущность функционирования системы защиты информации. Защита человека от опасной информации и от неинформированности в области информационной безопасности. Целостность, доступность и конфиденциальность информации. Классификация информации по видам тайны и степеням конфиденциальности. Понятия государственной тайны и конфиденциальной информации. Жизненные циклы конфиденциальной информации в процессе ее создания, обработки, передачи. Цели и задачи защиты информации. Основные понятия в области защиты информации. Элементы процесса менеджмента ИБ. Модель интеграции информационной безопасности в основную деятельность организации. Понятие Политики безопасности. Понятие угрозы безопасности информации. Системная классификация угроз безопасности информации. Каналы и методы несанкционированного доступа к информации. Уязвимости. Методы оценки уязвимости информации.
2	Методология защиты информации	Анализ существующих методик определения требований к защите информации.

		Параметры защищаемой информации и оценка факторов, влияющих на требуемый уровень защиты информации. Виды мер и основные принципы защиты информации. Организационная структура системы защиты информации. Законодательные акты в области защиты информации. Российские и международные стандарты, определяющие требования к защите информации. Система сертификации РФ в области защиты информации. Основные правила и документы системы сертификации РФ в области защиты информации. Основные механизмы защиты информации. Система защиты информации. Меры защиты информации, реализуемые в автоматизированных (информационных) системах. Программные и программно-аппаратные средства защиты информации. Инженерная защита и техническая охрана объектов информатизации. Организационно-распорядительная защита информации. Работа с кадрами и внутриобъектовый режим. Принципы построения организационно-распорядительной системы.

4. Оценочные средства

представлены в Приложении № 1 к РПД Фонд оценочных средств для проведения текущего контроля и итоговой аттестации

5. Учебно-методическое, информационное и материально-техническое обеспечение

а) 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. Мельников, А. В. Основы информационной безопасности: учебное пособие / А. В. Мельников, С. В. Зарубин. — Москва: Российский государственный университет правосудия, 2025. — 220 с. — ISBN 978-5-00209-188-1. — Текст: электронный // Цифровой образовательный ресурс IPR SMART: [сайт]. — URL: https://www.iprbookshop.ru/152309.html

3. Мирошников, А. И. Основы информационной безопасности и защита информации: учебное пособие / А. И. Мирошников, А. С. Сысоев. — Липецк: Липецкий государственный технический университет, ЭБС АСВ, 2022. — 107 с. — ISBN 978-5-00175-160-1. — Текст: электронный // Цифровой образовательный ресурс IPR SMART: [сайт]. — URL: https://www.iprbookshop.ru/128718.html

б) Информационное обеспечение

Ресурсы информационно-телекоммуникационной сети Интернет:

- http://window.edu.ru/ - единое окно доступа к образовательным ресурсам
- http://www.iprbookshop.ru/ - Электронно-библиотечная система IPRSmart (ЭБС IPRSmart) – электронная библиотека по всем отраслям знаний
- https://www.elibrary.ru/ - электронно-библиотечная система eLIBRARY.RU, крупнейшая в России электронная библиотека научных публикаций
- http://www.consultant.ru/ - справочная правовая система КонсультантПлюс
- https://www.garant.ru/ - справочная правовая система Гарант
- https://gufo.me/- справочная база энциклопедий и словарей
- https://reestr.digital.gov.ru/ - официальный сайт оператора единого реестра российских программ для электронных вычислительных машин и баз данных в информационно-телекоммуникационной сети «Интернет»

Программное обеспечение АНО ВО ИТУ, являющееся частью электронной информационно-образовательной среды и базирующееся на телекоммуникационных технологиях:

- Тренинговые и тестирующие программы;
- Интеллектуальные роботизированные системы оценки качества выполнения работ.
- Информационные и роботизированные системы, программные комплексы,
- Программное обеспечение для доступа к компьютерным обучающим, тренинговым и тестирующим программам:
- ПК «КОП»;
- ИР «Каскад».

Программное обеспечение, необходимое для реализации дисциплины:

Лицензионное программное обеспечение (в том числе, отечественного производства)

- Операционная система Windows Professional 10
- ПО браузер – приложение операционной системы, предназначенное для просмотра Web-страниц
- Платформа проведения аттестационных процедур с использованием каналов связи (отечественное ПО)
- Платформа проведения вебинаров (отечественное ПО)
- Информационная технология. Онлайн тестирование цифровой платформы Ровеб (отечественное ПО)
- Электронный информационный ресурс. Экспертный интеллектуальный информационный робот Аттестация асессоров (отечественное ПО)
- Информационная технология. Аттестационный интеллектуальный информационный

робот контроля оригинальности и профессионализма «ИИР КОП» (отечественное ПО)

- Электронный информационный ресурс «Личная студия обучающегося» (отечественное ПО)
- https://online.saby.ru/- Saby образовательный проект «Практическое применение программного обеспечения Saby» (отечественное ПО)

Свободно распространяемое программное обеспечение

- Мой Офис Веб-редакторы https://edit.myoffice.ru (отечественное ПО)
- ПО OpenOffice.Org Calc. http://qsp.su/tools/onlinehelp/about_license_gpl_russian.html
- ПО OpenOffice.Org.Base http://qsp.su/tools/onlinehelp/about_license_gpl_russian.html
- ПООpenOffice.org.Impress http://qsp.su/tools/onlinehelp/about_license_gpl_russian.html
- ПО OpenOffice.Org Writer http://qsp.su/tools/onlinehelp/about_license_gpl_russian.html
- ПО Open Office.org Draw http://qsp.su/tools/onlinehelp/about_license_gpl_russian.html
- ПО «Блокнот» - стандартное приложение операционной системы (MS Windows, Android и т.д.), предназначенное для работы с текстами.
- Пакеты прикладных программ: LibreOffice, Apache OpenOffice, Яндекс Документы/Таблицы/Презентации.

в) Материально-техническое обеспечение

1) Аудитория для проведения учебных занятий:

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

- Optoma DX322 Мультимедийный DLP проектор,
- DonView HB-82IN-H03 Интерактивная доска,
- Компьютерный стол и стул преподавателя,
- Компьютер преподавателя,
- Телевизор,
- Облучатель - рециркулятор настенный,
- Сплит-система,
- Шкаф книжный,
- Огнетушитель**.**

2) Многофункциональная аудитория для обучающихся с ограниченными возможностями здоровья, инвалидов (детей-инвалидов):

- Столы,
- Стулья,
- Классная доска меловая,
- Стол и стул преподавателя,
- Компьютер преподавателя,
- МФУ
- Компьютеры ученические,
- Индукционная петля "ИСТОК",

- Стол для МГН,
- Клавиатура адаптированная (шрифт Брайля),
- Мультимедийный проектор "EPSON",
- Экран,
- Лупа,
- Наушники,
- Колонки.
- Телевизор,
- Облучатель - рециркулятор настенный,
- Сплит-система,
- Шкаф книжный,
- Огнетушитель

3) Помещение для самостоятельной работы обучающихся:

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

- столы,
- стулья,
- персональные компьютеры с программным обеспечением и доступом в Интернет,

Рабочее место преподавателя:

- стол,
- стул,
- монитор,
- компьютер с программным обеспечением и доступом в Интернет;
- веб-камера,
- телевизор,
- классная доска,
- облучатель - рециркулятор настенный,
- сплит- система,
- шкаф книжный,
- огнетушитель.

6. Методические рекомендации по организации изучения дисциплины

Освоение дополнительной профессиональной программы - программы повышения квалификации проводится с применением электронного обучения и дистанционных образовательных технологий. Для планомерного изучения дисциплин обучающиеся знакомятся с учебным планом программы. Имеют календарный учебный график изучения дисциплин. Имеют примерные вопросы для самостоятельной работы, аттестации, пример индивидуальных заданий, список литературы.

Особенности организации образовательного процесса для обучающихся с ограниченными возможностями здоровья, инвалидов (детей-инвалидов) (в случае наличия таких категорий, обучающихся)

Образовательная программа может быть адаптирована для обучающихся с ограниченными возможностями здоровья, инвалидов (детей-инвалидов) (адаптивная образовательная программа). Адаптивная образовательная программа разрабатывается на основании личного заявления обучающегося (законного представителя) и рекомендаций психолого-медико-педагогической комиссии и/или справке медико-социальной экспертизы, индивидуальная программа реабилитации или абилитации.

При разработке адаптивной образовательной программы учитываются особые образовательные потребности обучающихся с ограниченными возможностями здоровья, инвалидов (детей-инвалидов), исходя из особенностей их психофизического развития, индивидуальных возможностей.

Обучающимся с ограниченными возможностями здоровья, инвалидам (детям-инвалидам) по их заявлению предоставляются специальные технические средства, программные средства и услуги ассистента (помощника), оказывающего необходимую техническую помощь.

При реализации адаптивной образовательной программы обучающимся с ограниченными возможностями здоровья, инвалидам (детям-инвалидам) предоставляются следующие возможности:

- использование специальных технических средств;
- обеспечение электронными образовательными ресурсами, использующими аудио сопровождение учебного материала;
- обеспечение электронными образовательными ресурсами с возможностью увеличения размера шрифта;
- обеспечение печатными образовательными ресурсами;
- особенности процедур аттестации.

При реализации адаптивной образовательной программы применяются следующие формы контроля и оценки результатов обучения обучающихся с ограниченными возможностями здоровья, инвалидов (детей-инвалидов) в зависимости от характера ограничений здоровья.

Для обучающихся с нарушением зрения:

- устная проверка;
- с использованием компьютера и специального программного обеспечения: работа с электронными образовательными ресурсами, тестирование, эссе;
- при возможности, письменная проверка с использованием шрифта Брайля, увеличенного шрифта, использование специальных технических средств: тестирование, индивидуальные задания, эссе.

Для обучающихся с нарушением слуха:

- письменная проверка: тестирование, индивидуальные задания, эссе;
- с использованием компьютера и специального программного обеспечения: работа с электронными образовательными ресурсами, тестирование, индивидуальные задания, эссе;
- при возможности, устная проверка с использованием специальных технических и программных средств.

Для обучающихся с нарушением опорно-двигательного аппарата:

- письменная проверка с использованием специальных технических средств: тестирование, индивидуальные задания, эссе;
- устная проверка с использованием специальных технических средств;
- с использованием компьютера и специального программного обеспечения: работа с электронными образовательными ресурсами, тестирование, индивидуальные задания, эссе;

При проведении текущей аттестации по дисциплине обеспечивается соблюдение следующих общих требований:

- проведение аттестации для обучающихся с ограниченными возможностями здоровья, инвалидов (детей-инвалидов) в одной аудитории совместно с обучающимися, не имеющими инвалидности и ОВЗ, если это не создает трудностей для обучающихся с ограниченными возможностями здоровья, инвалидов (детей-инвалидов) и иных обучающихся при прохождении аттестации;
- присутствие в аудитории ассистента (помощника), оказывающего обучающимся с ограниченными возможностями здоровья, инвалидам (детям-инвалидам) необходимую техническую помощь с учетом их индивидуальных особенностей (занять рабочее место, передвигаться, прочитать и оформить задание, общаться с экзаменатором);
- обеспечение возможности беспрепятственного доступа обучающихся с ограниченными возможностями здоровья, инвалидов (детей-инвалидов) в аудиторию, спортивный зал, санитарные и другие вспомогательные помещения.

По письменному заявлению обучающегося с ограниченными возможностями здоровья, инвалида (детей-инвалидов) продолжительность сдачи экзамена может быть увеличена по отношению к установленной продолжительности его сдачи:

- продолжительность сдачи экзамена, проводимого в письменной форме, - не более чем на 90 минут;
- продолжительность подготовки обучающегося к ответу на экзамене, проводимом в устной форме, - не более чем на 20 минут.

О необходимости обеспечения специальных условий для проведения аттестации обучающихся с ограниченными возможностями здоровья, инвалидов (детей-инвалидов), обучающийся должен сообщить письменно не позднее, чем за 10 дней до начала аттестации. К заявлению прилагаются документы, подтверждающие наличие у обучающегося индивидуальных особенностей (при отсутствии указанных документов в организации).

Приложение 1

Автономная некоммерческая организация высшего образования
«Информационно-технологический университет»
(АНО ВО ИТУ)

УТВЕРЖДАЮ

Ректор АНО ВО ИТУ Лиджиев Б.С.

Сведения об электронной подписи
Подписано: Лиджиев Борис Саранович
Должность: ректор
Пользователь: blidzhiev

Утверждено протоколом
заседания кафедры
Математики, информатики и
естественнонаучных дисциплин
№ 3 от 30.10.2025 г.

ДОПОЛНИТЕЛЬНАЯ ПРОФЕССИОНАЛЬНАЯ ПРОГРАММА ПОВЫШЕНИЯ КВАЛИФИКАЦИИ

«ЦИФРОВАЯ БЕЗОПАСНОСТЬ В ПРОФЕССИОНАЛЬНОЙ ДЕЯТЕЛЬНОСТИ»

ФОНД ОЦЕНОЧНЫХ СРЕДСТВ ДЛЯ ПРОВЕДЕНИЯ ТЕКУЩЕГО КОНТРОЛЯ И ИТОГОВОЙ АТТЕСТАЦИИПО ДИСЦИПЛИНЕ

«ОСНОВЫ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ»

г. Элиста, 2025

1. Общие положения

Контроль и оценка результатов освоения учебной дисциплины осуществляется в процессе изучения теоретических занятий с помощью тестирования, написания эссе по темам, выполнения практических заданий, а также выполнения обучающимися индивидуальных заданий. Оценка качества освоения программы включает текущий контроль успеваемости, итоговую аттестацию по окончанию изучения дисциплины.

2. Планируемые результаты обучения по дисциплине:

знать:

- сущность и понятие информационной безопасности, характеристику ее составляющих;
- место информационной безопасности в системе национальной безопасности страны;
- виды, источники и носители защищаемой информации;
- источники угроз безопасности информации и меры по их предотвращению;
- факторы, воздействующие на информацию при ее обработке в автоматизированных (информационных) системах;
- жизненные циклы информации ограниченного доступа в процессе ее создания, обработки, передачи;
- современные средства и способы обеспечения информационной безопасности;

уметь:

- классифицировать защищаемую информацию по видам тайны и степеням секретности;
- классифицировать основные угрозы безопасности информации;

владеть:

применения основных правил и документов систем сертификации Российской Федерации.

3. Оценочные средства для проведения промежуточной аттестации

Примерные темы эссе:

1. Развитие информационных технологий и роль информационной безопасности в современном мире.
2. Основные принципы и принципы информационной безопасности.
3. Типы угроз и атак на информационные системы и данные.
4. Роль человеческого фактора в информационной безопасности и методы обучения сотрудников.
5. Защита информационных систем от внешних угроз и атак.
6. Методы шифрования и протоколы безопасной передачи данных.
7. Защита от внутренних угроз и угроз со стороны сотрудников организации.
8. Разработка и применение политики информационной безопасности.
9. Защита от социальной инженерии и мошенничества.
10. Новые тенденции и вызовы в области информационной безопасности, такие как интернет вещей, облачные сервисы и искусственный интеллект

Пример индивидуального задания:

Тема: Анализ и оценка уязвимостей информационной системы.

1. Изучите основные концепции и принципы информационной безопасности, а также методы и инструменты анализа уязвимостей информационных систем.

2. Выберите информационную систему, которую вы будете анализировать, и определите ее функциональность, архитектуру, используемые технологии и предназначение.

3. Проведите исследование угроз, связанных с выбранной информационной системой, и определите потенциальные уязвимости.

4. Выполните анализ уязвимостей с использованием специализированных инструментов, таких как сканеры уязвимостей, проникновение в систему (pentesting), анализ кода и т. д.

5. Оцените риск, связанный с каждой уязвимостью, и определите потенциальные последствия для организации или пользователя информационной системы.

6. Разработайте план мероприятий по устранению уязвимостей и повышению безопасности информационной системы.

7. Реализуйте предлагаемые меры и протестируйте их эффективность, проведите повторный анализ уязвимостей для оценки уровня безопасности системы.

8. Составьте отчет о проведенном анализе уязвимостей и предложенных мерах по обеспечению безопасности информационной системы. В отчете укажите список обнаруженных уязвимостей, рекомендации по их устранению, оценку риска и последствий, а также результаты тестирования устранения уязвимостей.

9. Сформулируйте выводы о результатах анализа уязвимостей информационной системы и предложите рекомендации для улучшения ее безопасности. Обсудите меры, которые можно принять для предотвращения будущих уязвимостей и обеспечения надежной защиты информации.

10. Проведите анализ сетевой безопасности информационной системы и предложите меры по защите от сетевых атак, включая методы сетевого анализа и мониторинга, настройку брандмауэров, обнаружение вторжений и использование шифрования данных.

Примеры тестовых заданий:

1. Что такое информационная безопасность?

а) Защита информации от несанкционированного доступа, использования или разглашения.

б) Процесс обеспечения конфиденциальности, целостности и доступности информационных ресурсов.

в) Управление рисками, связанными с использованием информационных технологий.

г) Все вышеперечисленное.

2. Какие основные угрозы информационной безопасности существуют?

а) Вирусы и вредоносное программное обеспечение.

б) Социальная инженерия и фишинг.

в) Несанкционированный доступ и утечка данных.

г) Все вышеперечисленное.

3. Что означает аутентификация в контексте информационной безопасности?

а) Проверка подлинности пользователя или устройства перед предоставлением доступа к системе.

б) Метод шифрования данных для защиты их от несанкционированного доступа.

в) Процесс резервного копирования и восстановления данных.

г) Все вышеперечисленное.

4. Какие основные меры защиты можно применить для обеспечения информационной безопасности?

а) Использование сложных паролей и регулярное их изменение.

б) Регулярное обновление программного обеспечения и установка антивирусных программ.

в) Ограничение прав доступа пользователей и мониторинг сетевой активности.

г) Все вышеперечисленное.

5. Что такое политика информационной безопасности и какая роль ей отводится в организации?

а) Совокупность правил, процедур и руководящих принципов, которые регулируют безопасное использование информации.

б) Разработка и внедрение мер безопасности для защиты информационных систем.

в) Мониторинг соответствия действующих нормативных требований, связанных с безопасностью информации.

г) Все вышеперечисленное.

Примерные вопросы для самостоятельной работы:

1. Концепция ИБ: Раскройте содержание триады КИА (Конфиденциальность, Целостность, Доступность). Приведите по два конкретных примера нарушений каждого из этих принципов в реальной информационной системе (например, интернет-банкинг, корпоративная сеть).
2. Угрозы и уязвимости: В чем заключается ключевое различие между понятиями «угроза информационной безопасности», «уязвимость» и «риск»? Проиллюстрируйте ответ на примере атаки с использованием фишинга.
3. Криптография: Опишите принципиальные различия между симметричным и асимметричным шифрованием. Каковы основные преимущества и недостатки каждого подхода? В каких типовых сценариях они применяются (например, HTTPS, шифрование диска)?
4. Защита от вредоносного ПО: Составьте классификацию современных типов вредоносного программного обеспечения (вирусы, черви, трояны, шпионское ПО). Для каждого типа укажите основную цель атаки и основной вектор распространения.
5. Сетевые атаки и защита: Опишите механизмы атак типа «Отказ в обслуживании» и «Распределенный отказ в обслуживании». Какие существуют основные методы и средства защиты от таких атак на сетевом и организационном уровнях?
6. Аутентификация и управление доступом: Сравните три фактора аутентификации: «что-то знаешь» (пароль), «что-то имеешь» (токен) и «что-то есть» (биометрия). Проанализируйте достоинства и недостатки каждого с точки зрения удобства пользователя и надежности.
7. Политика безопасности: Что такое «Политика информационной безопасности» (ПИБ) организации? Из каких основных разделов она должна состоять? Объясните, почему формальная ПИБ является фундаментом для всей системы защиты, а не просто формальным документом.
8. Инциденты и расследование: Опишите основные этапы процесса реагирования на инциденты информационной безопасности (от обнаружения до восстановления). Почему этап

сбора и сохранения доказательств (компьютерная криминалистика) является критически важным?

9. Правовые основы: Какие основные российские законы и нормативные акты регулируют область информационной безопасности?

10. Человеческий фактор: Почему сотрудники организации часто считаются «слабым звеном» в системе информационной безопасности? Перечислите не менее трех мер (технических, организационных, обучающих), позволяющих минимизировать риски, связанные с человеческим фактором.

Отметка «зачтено» ставится, если слушатель: прослушал теоретические занятия, выполнил практических задания, показал при тестировании знание основных понятий, умение использовать и применять полученные знания при решении задач предметной области, набрав не менее 65%.

«Не зачтено»: если слушатель не прослушал лекции, не выполнил практические задания и при прохождении тестирования набрал менее 65%.

Критерии оценки ответов, обучающихся в ходе аттестации:

Оценка «отлично» выставляется при условии положительных ответов не менее 85%;

Оценка «хорошо» выставляется при условии положительных ответов не менее 75%;

Оценка «удовлетворительно» выставляется при условии положительных ответов не менее 65%;

Оценка «неудовлетворительно» выставляется при условии положительных ответов менее 65%.