

Документ подписан простой электронной подписью
Информация о владельце:
ФИО: Баламирзоев Назим Лиодинович
Должность: Ректор
Дата подписания: 2025.11.11
Уникальный программный ключ:
5cf0d6f89e80f49a334f6a4ba58e91f3326b9926

Министерство науки и высшего образования РФ

**Федеральное государственное бюджетное образовательное учреждение
высшего образования**

«Дагестанский государственный технический университет»

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ

Дисциплина Интеллектуальные системы информационной безопасности в
промышленных системах
наименование дисциплины по ОПОП

для направления подготовки 10.04.01 Информационная безопасность
код и полное наименование направления

по направленности Киберразведка и противодействие угрозам с применением
технологий искусственного интеллекта

факультет Компьютерных технологий и энергетики
наименование факультета, где ведется дисциплина

кафедра Информационная безопасность и программная инженерия
наименование кафедры, за которой закреплена дисциплина

Форма обучения очная курс 2 семестр (ы) 3
очная

Программа составлена в соответствии с требованиями ФГОС ВО по направлению подготовки 10.04.01 Информационная безопасность с учетом рекомендаций и ОПОП ВО по направлению подготовки и программе магистратуры «Киберразведка и противодействие угрозам с применением технологий искусственного интеллекта»

Разработчик 
(подпись)

Качаева Г.И., к.э.н.
(ФИО уч. степень, уч. звание)

« 02 » февраля 2026 г.

Зав. кафедрой, за которой закреплена дисциплина


(подпись)

Качаева Г.И., к.э.н.
(ФИО уч. степень, уч. звание)

« 03 » февраля 2026 г.

Программа одобрена на заседании выпускающей кафедры информационной безопасности и программной инженерии от « 05 » февраля 2026 года, протокол № 6/1

Зав. выпускающей кафедрой по данному направлению подготовки


(подпись)

Качаева Г.И. к.э.н.
(ФИО уч. степень, уч. звание)

« 05 » февраля 2026 г.

Программа одобрена на заседании Методического совета факультета компьютерных технологий и энергетики от « 10 » февраля 2026 г., протокол № 5/1

Председатель Методического совета факультета КТиЭ


(подпись)

Исабекова Т.И., к.ф.-м.н., доцент
(ФИО уч. степень, уч. звание)

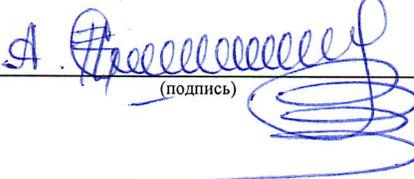
« 10 » февраля 2026 г.

Декан факультета 
(подпись)

Т.А. Рагимова
(ФИО)

Начальник УО 
(подпись)

Л.Н. Мусаева
(ФИО)

Проректор по УР 
(подпись)

А.Ф. Демирова
(ФИО)

Содержание

1.	ОБЩАЯ ХАРАКТЕРИСТИКА РАБОЧЕЙ ПРОГРАММЫ ДИСЦИПЛИНЫ.....	4
1.1.	Место дисциплины в структуре ОПОП.....	4
1.2.	Цели и задачи освоения дисциплины	4
1.3.	Компетенции обучающегося, формируемые в результате освоения дисциплины	4
2.	СТРУКТУРА И СОДЕРЖАНИЕ ДИСЦИПЛИНЫ	6
2.1.	Объем дисциплины и виды учебной работы	6
2.2.	Содержание дисциплины «Интеллектуальные системы информационной безопасности в промышленных системах»	7
3.	УСЛОВИЯ РЕАЛИЗАЦИИ ПРОГРАММЫ ДИСЦИПЛИНЫ	11
3.1.	Материально-техническое обеспечение.....	11
3.2.	Учебно-методическое и информационное обеспечение программы	11
3.2.1.	Печатные издания	12
3.2.2.	Основные электронные издания	12
4.	КОНТРОЛЬ И ОЦЕНКА РЕЗУЛЬТАТОВ ОСВОЕНИЯ ДИСЦИПЛИНЫ.....	13

1. ОБЩАЯ ХАРАКТЕРИСТИКА РАБОЧЕЙ ПРОГРАММЫ ДИСЦИПЛИНЫ

1.1. Место дисциплины в структуре ОПОП

Дисциплина «Интеллектуальные системы информационной безопасности в промышленных системах» входит в часть, формируемую участниками образовательных отношений учебного плана по программе магистратуры 10.04.01 Информационная безопасность, направленность «Киберразведка и противодействие угрозам с применением технологий искусственного интеллекта».

Предшествующими дисциплинами, формирующими начальные знания, являются: интеллектуальные системы и технологии, технологии машинного обучения в кибербезопасности, теория обнаружения вторжений с применением ИИ, системы мониторинга и управления инцидентами ИБ, система для сбора событий и логов, моделирование бизнес-процессов, анализ защищенности систем искусственного интеллекта, защищенные информационные системы.

Дисциплина «Интеллектуальные системы информационной безопасности в промышленных системах» является основополагающей для изучения следующих дисциплин: Производственная (проектно-технологическая) практика, Преддипломная практика, Государственная итоговая аттестация.

1.2. Цели и задачи освоения дисциплины

Дисциплина «Интеллектуальные системы информационной безопасности в промышленных системах» способствует формированию у обучающихся компетенций, предусмотренных данной рабочей программой в соответствии с требованиями ФГОС ВО и ОПОП ВО по направлению подготовки 10.04.01 Информационная безопасность с учетом специфики направленности подготовки «Киберразведка и противодействие угрозам с применением технологий искусственного интеллекта».

1.3. Компетенции обучающегося, формируемые в результате освоения дисциплины

В результате освоения дисциплины «Интеллектуальные системы информационной безопасности в промышленных системах» обучающийся должен овладеть следующими компетенциями:

Таблица 1.

Код и наименование компетенции	Код и наименование индикаторов достижения компетенции
ПК- 1 Способен разрабатывать и применять процедуры и интеллектуальные средства информационно-аналитических систем поддержки принятия решений по обеспечению информационной безопасности	ПК-1.2 Способен интерпретировать и использовать результаты решения информационно-аналитических задач обеспечения информационной безопасности
	ПК-1.3 Способен разрабатывать информационно-аналитические системы в сфере информационной безопасности
ПК-2 Способен выполнять мониторинг и ситуационный анализ обстановки в сфере информационной безопасности	ПК-2.1 Способен формализовывать задачи информационно-аналитической поддержки принятия решений в сфере информационной безопасности
ПК-3 Способен исследовать и разрабатывать архитектуры систем искусственного интеллекта для различных предметных областей на основе	ПК-3.1 Выбирает комплексы методов и инструментальных средств искусственного интеллекта для решения задач в зависимости от особенностей предметной области

комплексов методов и инструментальных средств систем искусственного интеллекта	
ПК-5 Способен разрабатывать и модернизировать программное и аппаратное обеспечение технологий и систем искусственного интеллекта с учетом требований информационной безопасности в различных предметных областях	ПК-5.1 Разрабатывает программное и аппаратное обеспечение технологий и систем искусственного интеллекта для решения профессиональных задач с учетом требований информационной безопасности в различных предметных областях
ПК-7 Способен руководить проектами по созданию комплексных систем искусственного интеллекта	ПК-7.1 Руководит разработкой архитектуры комплексных систем искусственного интеллекта

2. СТРУКТУРА И СОДЕРЖАНИЕ ДИСЦИПЛИНЫ

2.1. Объем дисциплины и виды учебной работы

Таблица 2.

Вид учебной работы	Форма обучения
	очная
Объем образовательной программы дисциплины (ЗЕТ/ в часах)	4/144
В том числе:	Объем в часах
Лекции	17
Практические занятия	
Лабораторные занятия	34
Самостоятельная работа	57
Курсовой проект (работа), семестр	-
Промежуточная аттестация в форме экзамена, семестр	3 семестр
Часы на экзамен	36

2.2. Содержание дисциплины

Наименование разделов и тем	Содержание учебного материала и формы организации деятельности обучающихся	Объем в часах	Коды компетенций, формированию которых способствует элемент программы
Раздел 1. Основные понятия и определения интеллектуальных систем			
Тема 1.1 Введение в интеллектуальные системы информационной безопасности	Понятие данных, знаний, информации. Характеристика явного и неявного, предметного и проблемного видов знаний.	2	ПК-1; ПК-2; ПК-3
	в том числе лабораторных занятий:	4	
	Лабораторная работа № 1. Построение модели угроз для виртуальной мини-АСУ ТП. Использование методики STRIDE или MITRE ATT&CK for ICS для идентификации уязвимостей SCADA, HMI, контроллеров.		
	Самостоятельная работа обучающихся: Сравнительный анализ стандартов промышленной кибербезопасности: МЭК 62443 vs. NIST SP 800-82 vs. требования ФСТЭК России.	6	
Тема 1.2 Системы с интеллектуальной обратной связью и интеллектуальными интерфейсами	Интеллектуальная обратная связь и интеллектуальный интерфейс. Классификация интеллектуальных информационных систем.	2	ПК-1; ПК-2; ПК-3
	в том числе лабораторных занятий:	4	
	Лабораторная работа № 2. Настройка сбора и парсинга данных промышленного протокола с использованием ELK-стека или Wazuh.		
	Самостоятельная работа обучающихся: Исследование реальных инцидентов кибербезопасности на промышленных объектах. Разбор векторов атак, последствий и уроков.	6	
Тема 1.3 Автоматизированные системы распознавания образов	Зрительное восприятие реального мира, машинное зрение; распознавание образов; интеллектуальные роботы, зрительные системы интеллектуальных роботов; специальное программное обеспечение.	2	ПК-1; ПК-2; ПК-3
	в том числе лабораторных занятий:	4	

	Лабораторная работа № 3. Разработка простого детектора аномалий для технологического параметра на основе автоэнкодера. Обучение на нормальных данных, выявление аномалий в тестовом наборе.		
	Самостоятельная работа обучающихся: Обзор рынка решений по интеллектуальной промышленной кибербезопасности.	6	
Тема 1.4 Методы поддержки принятия решений	Классификация методов решения задач. Методы решения задач в системах, основанных на знаниях	2	ПК-1; ПК-2; ПК-3
	в том числе лабораторных занятий:	4	
	Лабораторная работа № 4. Создание базы корреляционных правил для SIEM для детектирования атаки на PLC.		
	Самостоятельная работа обучающихся: Изучение промышленных протоколов и их уязвимостей с использованием открытых ресурсов.	6	
Тема 1.5 Экспертные системы	Экспертные системы. Структура. Назначение. Технологии разработки. Представление знаний в экспертной системе. Методы экспертных оценок. Обработка экспертных оценок. Экспертные системы с неопределенными знаниями.	2	ПК-1; ПК-2; ПК-3
	в том числе лабораторных занятий:	4	
	Лабораторная работа № 5. Моделирование и обнаружение атаки "Man-in-the-Middle" на канал OPC UA с помощью анализа сетевого трафика и методов ML.		
	Самостоятельная работа обучающихся: Разработка концепции интеллектуального модуля для обнаружения атак на систему телеметрии энергосети.	6	
Тема 1.6 Эволюционные вычисления	Понятие «эволюционные вычисления». Эволюционное программирование. Генетические алгоритмы. Эволюционные стратегии.	2	ПК-1; ПК-2; ПК-3
	в том числе лабораторных занятий:	4	
	Лабораторная работа № 6. Прогнозирование параметра технологического процесса с использованием LSTM-сети. Оценка точности и использование отклонения прогноза от реальных данных как индикатора атаки.		

	Самостоятельная работа обучающихся: Написание скрипта для симуляции нормального и аномального сетевого трафика Modbus TCP для последующего обучения ML-модели.	6	
Тема 1.7 Языки и средства разработки интеллектуальных систем	Языки и средства разработки интеллектуальных систем	2	ПК-1; ПК-2; ПК-3; ПК-5; ПК-7
	в том числе лабораторных занятий:	4	
	Лабораторная работа № 7. Разработка сценария автоматического реагирования в SOAR-платформе на инцидент "несанкционированный доступ к НМИ". Сценарий должен включать оповещение, сбор артефактов и изоляцию НМИ.		
	Самостоятельная работа обучающихся: Анализ компромисса между производительностью и безопасностью при внедрении систем ИИ на уровне контроллеров.	6	
Тема 1.8 Методы идентификации и аутентификации пользователей	Управление доступом. Регистрация действий пользователей. Контроль доступа пользователей к ресурсам ИС.	2	ПК-1; ПК-2; ПК-3; ПК-5; ПК-7
	в том числе лабораторных занятий:	4	
	Лабораторная работа № 8. Анализ защищенности edge-устройства и настройка на нем lightweight ML-модели для локального детектирования аномалий.		
	Самостоятельная работа обучающихся: Проектирование схемы сегментации промышленной сети с учетом размещения компонентов интеллектуальной системы ИБ.	7	
Раздел 2. Интеллектуальные системы информационной безопасности в промышленных			
Тема 2.1 Управление жизненным циклом и проектами внедрения интеллектуальных систем ИБ в промышленности.	Оценка ROI, управление рисками внедрения, взаимодействие с технологами и инженерами, пилотные зоны.	1	ПК-1; ПК-2; ПК-3; ПК-5; ПК-7
	в том числе лабораторных занятий:	2	
	Лабораторная работа № 9. Командная работа: проектирование архитектуры интеллектуальной системы ИБ для заданного объекта. Подготовка презентации с обоснованием выбора методов, инструментов и оценкой рисков.		
	Самостоятельная работа обучающихся: Подготовка тезисов доклада на научно-техническую конференцию на тему "Вызовы применения ИИ для защиты Industry 4.0: от аналитики к автономному реагированию".	8	
Итого за 3 семестр:			

Лекции	17	
Лабораторные работы	34	
Самостоятельная работа	57	
Промежуточная аттестация в форме экзамена	36	
Всего:	144	

3. УСЛОВИЯ РЕАЛИЗАЦИИ ПРОГРАММЫ ДИСЦИПЛИНЫ

3.1. Материально-техническое обеспечение

Материально-техническое обеспечение дисциплины «Интеллектуальные системы информационной безопасности в промышленных системах» включает:

Наименование помещения	Перечень основного оборудования
Лаборатория защиты информации	Рабочее место преподавателя; Посадочные места по количеству обучающихся; Автоматизированные рабочие места (ПК в сборе) с доступом в сеть Интернет; Интерактивная система в составе: проектор интерактивная доска Программное и программно-аппаратное обеспечение: Система защиты информации от НСД «Страж NT»; Dallas Lock - система защиты информации от несанкционированного доступа в процессе хранения и обработки; Программный комплекс по предотвращению утечек данных (DLP) Кибер Протега Электронный ключ GUARDANT ID; Электронный ключ Rutoken; СЗИ НСД Аккорд-АМДЗ. Базовый набор функций, шина PCI-express, прошивка с поддержкой UEFI (арт.Р79UGX); Право на использование СПО «Аккорд-Х» OpenPLC, Node RED, SCADA BR, CogniDAQ; Wireshark (с плагинами для Modbus, DNP3, IEC 60870 5 104)
Аудитория для проведения занятий лекционного типа	Рабочее место преподавателя; Посадочные места по количеству обучающихся; Автоматизированные рабочие места (ПК в сборе) с доступом в сеть Интернет; Интерактивная система в составе: проектор, интерактивная доска
Аудитория для самостоятельной работы обучающихся:	Автоматизированные рабочие места (ПК в сборе) с доступом в сеть Интернет; Интерактивная система в составе: проектор, интерактивная доска

3.2. Учебно-методическое и информационное обеспечение программы

Для реализации программы библиотечный фонд образовательной организации имеет печатные и/или электронные образовательные и информационные ресурсы для использования в образовательном процессе. При формировании библиотечного фонда образовательной организации выбирается не менее одного издания из перечисленных ниже печатных изданий и (или) электронных изданий в качестве основного, при этом список может быть дополнен новыми изданиями

3.2.1. Печатные издания

Основная литература:

1. Митяков, Е. С. Искусственный интеллект и машинное обучение: учебное пособие для вузов / Е. С. Митяков, А. Г. Шмелева, А. И. Ладынин. — 2-е изд., стер. — Санкт-Петербург: Лань, 2026. — 252 с. — ISBN 978-5-507-51198-3. — Текст: электронный // Лань: электронно-библиотечная система. — URL: <https://e.lanbook.com/book/507451>
2. Остроух, А. В. Интеллектуальные информационные системы и технологии: учебное пособие / А. В. Остроух, А. Б. Николаев. — 3-е изд., стер. — Санкт-Петербург: Лань, 2023. — 308 с. — ISBN 978-5-507-48511-6. — Текст: электронный // Лань: электронно-библиотечная система. — URL: <https://e.lanbook.com/book/354536>
3. Хабаров, С. П. Интеллектуальные системы и технологии. Роевые алгоритмы: инновационные подходы к оптимизации: учебное пособие / С. П. Хабаров, А. М. Заяц; ответственный редактор С. П. Хабаров. — Санкт-Петербург: СПбГЛТУ, 2024. — 190 с. — ISBN 978-5-9239-1499-3. — Текст: электронный // Лань: электронно-библиотечная система. — URL: <https://e.lanbook.com/book/454406>

Дополнительные источники:

1. Ермакова, А. Н. Управление ИТ-проектами. Ч.II: учебник / А. Н. Ермакова, С. В. Богданова. — Ставрополь: АГРУС, 2024. — 220 с. — Текст: электронный // Цифровой образовательный ресурс IPR SMART: [сайт]. — URL: <https://www.iprbookshop.ru/156621.html>
2. Шелухин, О. И. Системы обнаружения вторжений в компьютерные сети: учебное пособие / О. И. Шелухин, А. Н. Руднев, А. В. Савелов. — Москва: Московский технический университет связи и информатики, 2013. — 88 с. — Текст: электронный // Цифровой образовательный ресурс IPR SMART: [сайт]. — URL: <https://www.iprbookshop.ru/63360.html>
3. Практикум по дисциплине Системы обнаружения вторжений в инфокоммуникациях / составители В. А. Мочалов. — Москва: Московский технический университет связи и информатики, 2014. — 28 с. — Текст: электронный // Цифровой образовательный ресурс IPR SMART: [сайт]. — URL: <https://www.iprbookshop.ru/61545.html>

3.2.2. Основные электронные издания

1. Министерство науки и высшего образования Российской Федерации <https://minobrnauki.gov.ru/>
2. Российская академия наук <https://www.ras.ru/>
3. Российский фонд фундаментальных исследований (Российский центр научной информации) <https://www.rfbr.ru/>

4. КОНТРОЛЬ И ОЦЕНКА РЕЗУЛЬТАТОВ ОСВОЕНИЯ ДИСЦИПЛИНЫ

Контроль и оценка результатов освоения дисциплины осуществляется преподавателем в процессе проведения лабораторных работ, тестирования, а также выполнения обучающимися индивидуальных заданий.

Результаты обучения	Критерии оценки	Методы оценки
<p>- Способен интерпретировать и использовать результаты решения информационно-аналитических задач обеспечения информационной безопасности</p> <p>- Способен разрабатывать информационно-аналитические системы в сфере информационной безопасности</p> <p>- Способен формализовывать задачи информационно-аналитической поддержки принятия решений в сфере информационной безопасности</p> <p>- Выбирает комплексы методов и инструментальных средств искусственного интеллекта для решения задач в зависимости от особенностей предметной области</p> <p>- Разрабатывает программное и аппаратное обеспечение технологий и систем искусственного интеллекта для решения профессиональных задач с учетом требований информационной безопасности в различных предметных областях</p> <p>- Руководит разработкой архитектуры комплексных систем искусственного интеллекта</p>	<p><i>Шкала оценивания для экзамена</i></p> <p>«Отлично» Показывает высокий уровень сформированности компетенций, т.е.:</p> <ul style="list-style-type: none"> - демонстрирует высокое и прочное освоение материала; - исчерпывающе, четко, последовательно, грамотно и логически стройно излагает теоретический материал; - правильно формирует определения; - демонстрирует умения самостоятельной работы с нормативно-правовой литературой; - умеет делать выводы по излагаемому материалу. <p>«Хорошо» Показывает достаточный уровень сформированности компетенций, т.е.:</p> <ul style="list-style-type: none"> - демонстрирует достаточно полное знание материала, основных теоретических положений; - достаточно последовательно, грамотно и логически стройно излагает теоретический материал; - демонстрирует умения ориентироваться в нормативно-правовой литературе; - умеет делать достаточно обоснованные выводы по излагаемому материалу. <p>«Удовлетворительно» Показывает пороговый уровень сформированности компетенций, т.е.:</p> <ul style="list-style-type: none"> - демонстрирует общее знание изучаемого материала; - испытывает затруднения при ответах на дополнительные вопросы; - знает основную рекомендуемую литературу; - умеет строить ответ в соответствии со структурой излагаемого материала. <p>«Неудовлетворительно» Ставится в случае:</p> <ul style="list-style-type: none"> - незнания значительной части программного материала; - невладения понятийным аппаратом дисциплины; - допущения существенных ошибок при изложении учебного материала; - неумения строить ответ в соответствии со структурой излагаемого вопроса; - неумения делать выводы по излагаемому материалу. 	<p>Текущий контроль при проведении:</p> <ul style="list-style-type: none"> - письменного/устного опроса; - тестирования; - оценки результатов самостоятельной работы (докладов, рефератов). <p>Промежуточная аттестация в форме:</p> <ul style="list-style-type: none"> - экзамена, - письменных/устных ответов, - тестирования.

Специальные условия инвалидам и лицам с ограниченными возможностями здоровья (ОВЗ)

Обучающиеся из числа инвалидов и лиц с ОВЗ обеспечены печатными и (или) электронными образовательными ресурсами в формах, адаптированных к ограничениям их здоровья.

Специальные условия обучения и направления работы с инвалидами и лицами с ОВЗ определены на основании:

- Федерального закона от 29.12.2012 №273-ФЗ «Об образовании в Российской Федерации»;
- Федерального закона от 24.11.1995 № 181-ФЗ «О социальной защите инвалидов в Российской Федерации»;
- приказа Минобрнауки России от 06.04.2021 № 245 «Об утверждении Порядка организации и осуществления образовательной деятельности по образовательным программам высшего образования - программам бакалавриата, программам специалитета, программам магистратуры»;
- методических рекомендаций по организации образовательного процесса для обучения инвалидов и лиц с ограниченными возможностями здоровья в образовательных организациях высшего образования, в том числе оснащенности образовательного процесса, утвержденных Минобрнауки России 08.04.2014 № АК-44/05вн).

Под специальными условиями для получения образования обучающихся с ОВЗ понимаются условия обучения, воспитания и развития, включающие в себя использование при необходимости адаптированных образовательных программ и методов обучения и воспитания, специальных учебников, учебных пособий и дидактических материалов, специальных технических средств обучения коллективного и индивидуального пользования, предоставление услуг ассистента (помощника), оказывающего необходимую помощь, проведение групповых и индивидуальных коррекционных занятий, обеспечение доступа в здания ДГТУ и другие условия, без которых невозможно или затруднено освоение ОПОП обучающихся с ОВЗ.

Обучение в рамках учебной дисциплины обучающихся с ОВЗ осуществляется ДГТУ с учетом особенностей психофизического развития, индивидуальных возможностей и состояния здоровья таких обучающихся.

Обучение по учебной дисциплине обучающихся с ОВЗ может быть организовано как совместно с другими обучающимися, так и в отдельных группах.

В целях доступности обучения по дисциплине обеспечивается:

1) для лиц с ограниченными возможностями здоровья по зрению:

- наличие альтернативной версии официального сайта ДГТУ в сети «Интернет» для слабовидящих;
- весь необходимый для изучения материал, согласно учебному плану (в том числе, для обучающихся по индивидуальным учебным планам) предоставляется в электронном виде на диске.
- индивидуальное равномерное освещение не менее 300 люкс;
- присутствие ассистента, оказывающего обучающемуся необходимую помощь;
- обеспечение возможности выпуска альтернативных форматов печатных материалов (крупный шрифт или аудиофайлы);
- обеспечение доступа обучающегося, являющегося слепым и использующего собаку-проводника, к зданию ДГТУ.

2) для лиц с ОВЗ по слуху:

- наличие микрофонов и звукоусиливающей аппаратуры коллективного пользования (аудиоколонки);

3) для лиц с ОВЗ, имеющих нарушения опорно-двигательного аппарата, материально-технические условия должны обеспечивать возможность беспрепятственного доступа обучающихся в учебные помещения, столовые, туалетные и другие помещения организации, а также пребывания в указанных помещениях (наличие пандусов, поручней, расширенных дверных проемов и других приспособлений).

Перед началом обучения могут проводиться консультативные занятия, позволяющие студентам с ОВЗ адаптироваться к учебному процессу.

В процессе ведения учебной дисциплины научно-педагогическим работникам рекомендуется использование социально-активных и рефлексивных методов обучения, технологий социокультурной реабилитации с целью оказания помощи обучающимся с ОВЗ в установлении полноценных межличностных отношений с другими обучающимися, создании комфортного психологического климата в учебной группе.

Особенности проведения текущей и промежуточной аттестации по дисциплине для обучающихся с ОВЗ устанавливаются с учетом индивидуальных психофизических особенностей (устно, письменно на бумаге, письменно на компьютере, в форме тестирования и др.). При необходимости предоставляется дополнительное время для подготовки ответа на зачете или экзамене