**Министерство науки и высшего образования РФ**

**Федеральное государственное бюджетное образовательное учреждение высшего образования**

**«Дагестанский государственный технический университет»**

# РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ

Дисциплина Системы мониторинга и управления инцидентами информационной безопасности
наименование дисциплины по ОПОП

для направления подготовки 10.04.01 Информационная безопасность
код и полное наименование направления

по направленности Кибербразведка 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 1 семестр (ы) 2 .
очная

г. Махачкала – 2026

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 «Кибербразведка и противодействие угрозам с применением технологий искусственного интеллекта»

**Разработчик** _____ Качаева Г.И., к.э.н.
( подпись) (ФИО уч. степень, уч. звание)

« 02 » февраля 2026 г.

**Зав. кафедрой, за которой закреплена дисциплина**

_____ Качаева Г.И., к.э.н.
(подпись) (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**

_____ Качаева Г.И. к.э.н.
(подпись) (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**

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

« 10 » февраля 2026 г.

**Декан факультета** _____ Т.А. Рагимова
(подпись) (ФИО)

**Начальник УО** _____ Л.Н. Мусаева
(подпись) (ФИО)

**Проректор по УР** _____ А.Ф. Демирова
(подпись) (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 ..... 5
2.1. Объем дисциплины и виды учебной работы ..... 5
2.2. Содержание дисциплины «Системы мониторинга и управления инцидентами информационной безопасности» ..... 6
3. УСЛОВИЯ РЕАЛИЗАЦИИ ПРОГРАММЫ ДИСЦИПЛИНЫ ..... 12
3.1. Материально-техническое обеспечение ..... 12
3.2. Учебно-методическое и информационное обеспечение программы ..... 12
3.2.1. Печатные издания ..... 12
3.2.2. Основные электронные издания ..... 13
4. КОНТРОЛЬ И ОЦЕНКА РЕЗУЛЬТАТОВ ОСВОЕНИЯ ДИСЦИПЛИНЫ ..... 14

# 1. ОБЩАЯ ХАРАКТЕРИСТИКА РАБОЧЕЙ ПРОГРАММЫ ДИСЦИПЛИНЫ

## 1.1. Место дисциплины в структуре ОПОП

Дисциплина «Системы мониторинга и управления инцидентами информационной безопасности» входит в часть, формируемую участниками образовательных отношений учебного плана по программе магистратуры 10.04.01 Информационная безопасность, направленность «Кибербразведка и противодействие угрозам с применением технологий искусственного интеллекта»

Предшествующими дисциплинами, формирующими начальные знания, являются: защищенные информационные системы, технологии обеспечения информационной безопасности, система для сбора событий и логов, теория обнаружения вторжений с применением ИИ, технологии машинного обучения в кибербезопасности, библиотеки машинного обучения, моделирование бизнес-процессов.

Дисциплина «Системы мониторинга и управления инцидентами информационной безопасности» является основополагающей для изучения следующих дисциплин: Технологии извлечения знаний из больших данных, Библиотеки машинного обучения, Технологии машинного обучения в кибербезопасности, Управление проектами интеллектуальных информационных систем, Теория обнаружения вторжений с применением искусственного интеллекта Интеллектуальные системы информационной безопасности в промышленных системах, Интеллектуальные системы информационной безопасности в здравоохранении, Анализ защищенности систем искусственного интеллекта, Моделирование бизнес-процессов.

## 1.2. Цели и задачи освоения дисциплины

Дисциплина «Системы мониторинга и управления инцидентами информационной безопасности» 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 «Кибербразведка и противодействие угрозам с применением технологий искусственного интеллекта».

## 1.3. Компетенции обучающегося, формируемые в результате освоения дисциплины

В результате освоения дисциплины «Системы мониторинга и управления инцидентами информационной безопасности» 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-1.3 Способен разрабатывать информационно-аналитические системы в сфере информационной безопасности |
| 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) | 3/108 |
| **В том числе:** | **Объем в часах** |
| Лекции | 34 |
| Практические занятия | |
| Лабораторные занятия | 34 |
| Самостоятельная работа | 40 |
| Курсовой проект (работа), семестр | - |
| Промежуточная аттестация в форме зачета**,** семестр | 2 семестр |
| Часы на экзамен | - |

## 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. Технические решения мониторинга информационной безопасности** | | | |
| **Тема 1.1 Обзор современных технических решений мониторинга информационной безопасности** | Основные понятия и определения. Классификация технических средств мониторинга ИБ. Описание процесса сбора и обработки сведений в реальном времени. Основные компоненты ИАС мониторинга. | **2** | ПК-1; ПК-7 |
| | **в том числе лабораторных занятий:** | **2** | |
| | Лабораторная работа № 1.<br>Развертывание тестовой инфраструктуры SIEM Настройка серверных компонентов | | |
| | **Самостоятельная работа обучающихся:**<br>Сравнительный анализ коммерческих и open-source SIEM решений. | **2** | |
| **Тема 1.2 Источники сведений системы мониторинга информационной безопасности** | Основные источники сведений системы мониторинга. DLP-системы, IDS-системы, журналы событий домена. Достоинства и недостатки. | **2** | ПК-1; ПК-7 |
| | **в том числе лабораторных занятий:** | **2** | |
| | Лабораторная работа № 2.<br>Настройка агентов и сбор логов с различных источников . Конфигурирование файлов beats или Wazuh agent. | | |
| | **Самостоятельная работа обучающихся:**<br>Исследование модели зрелости SOC. Определение этапов развития и ключевых показателей для каждого уровня. | **2** | |
| **Тема 1.3 Описание технического решения мониторинга Log Management** | Log Management - специализированное решение типа Elastic Stack. Описание технологии. Достоинства и недостатки. | **2** | ПК-1; ПК-7 |
| | **в том числе лабораторных занятий:** | **2** | |
| | Лабораторная работа № 3.<br>Создание парсеров и нормализация пользовательских логов. Написание grok-фильтров для Logstash или правил декодирования для Wazuh. | | |

| | | | |
|---|---|---|---|
| | **Самостоятельная работа обучающихся:**<br>Глубокий разбор стандарта NIST SP 800-61. Конспектирование основных этапов и рекомендаций. | **4** | |
| **Тема 1.4 Централизованное хранилище журналов событий различных источников** | Определение перечня источников, настроек аудита, полей событий и способов сбора; подключение всех типов источников для анализа. | **2** | ПК-1; ПК-7 |
| | **в том числе лабораторных занятий:** | **2** | |
| | Лабораторная работа № 4.<br>Разработка правил корреляции для детектирования брутфорс-атаки. Написание правил на языке SIEM с использованием временных окон. | | |
| | **Самостоятельная работа обучающихся:**<br>Обзор рынка Threat Intelligence Feeds. Анализ форматов данных, актуальности и применимости для автоматизации в SOAR. | **2** | |
| **Тема 1.5 Описание технического решения мониторинга SIEM-системы** | Примеры пакетов экспертизы: обнаружение продвинутых атак на Active Directory, аномалий в активности пользователей, атак с тактиками по модели MITRE ATT&CK, аномалий при удаленной работе. | **2** | ПК-1; ПК-7 |
| | **в том числе лабораторных занятий:** | **2** | |
| | Лабораторная работа № 5.<br>Создание правила для обнаружения последовательности действий по MITRE ATT&CK. Детектирование попыток использования PsExec или WMI после компрометации. | | |
| | **Самостоятельная работа обучающихся:**<br>Изучение тактик MITRE ATT&CK и подготовка матрицы детекторов для 3-х выбранных тактик. Сопоставление техник атак с возможными правилами корреляции в SIEM. | **2** | |
| **Тема 1.6 Выявление инцидентов с помощью MaxPatrol SIEM** | Описание системы мониторинга. Создание новых правил, обновление параметров сбора и обработки событий ИБ. | **2** | ПК-1; ПК-7 |
| | **в том числе лабораторных занятий:** | **2** | |
| | Лабораторная работа № 6.<br>Интеграция SIEM с внешним Threat Intelligence Feed. Настройка обогащения событий IoC. | | |
| | **Самостоятельная работа обучающихся:**<br>Написание парсера для нестандартного лог-файла приложения и создание тестовых данных для его проверки. | **2** | |

| | | | |
|---|---|---|---|
| **Тема 1.7 Описание технического решения Threat Intelligence** | Этапы процесса кибербразведки: планирование, сбор информации, обработка собранных данных, подготовка данных для отчета. | **2** | ПК-1; ПК-7 |
| | **в том числе лабораторных занятий:** | **2** | |
| | Лабораторная работа № 7.<br>Разработка простого ML-скрипта для аномалий входа в систему и интеграция его результатов в SIEM. Использование scikit-learn для обнаружения выбросов и генерация кастомного лога. | | |
| | **Самостоятельная работа обучающихся:**<br>Проектирование Playbook для реагирования на инцидент утечки данных. Описание шагов: идентификация источника, оценка объема, блокировка канала утечки, уведомление. | **2** | |
| **Тема 1.8 Автоматизация процессов кибербразведки на основе решений класса Threat Intelligence Platform** | Описание платформы Anomali, позволяющая получать фиды в открытых стандартах обмена информацией о киберугрозах STIX. | **2** | ПК-1; ПК-7 |
| | **в том числе лабораторных занятий:** | **2** | |
| | Лабораторная работа № 8.<br>Развертывание и базовое конфигурирование SOAR-платформы. Установка, настройка интеграций. | | |
| | **Самостоятельная работа обучающихся:**<br>Анализ кейса реального крупного инцидента. Реконструкция того, как можно было бы обнаружить и остановить атаку с помощью корректно настроенного SIEM/SOAR. | **2** | |
| **Раздел 2. Применение искусственного интеллекта при управлении информационной** | | | |
| **Тема 2.1 Организация системы безопасностью мониторинга информационной безопасности** | Компоненты системы мониторинга информационной безопасности и их функции. Программно-технический компонент. Документационный компонент. Кадровый компонент. | **2** | ПК-1; ПК-7 |
| | **в том числе лабораторных занятий:** | **2** | |
| | Лабораторная работа № 9.<br>Создание простого Playbook для автоматического реагирования на обнаружение вредоносного файла. . | | |
| | **Самостоятельная работа обучающихся:**<br>Исследование методов снижения ложных срабатываний в SIEM. Анализ подходов: тонкая настройка правил, контекстное обогащение, применение ML. | **2** | |

| | | | |
|---|---|---|---|
| **Тема 2.2 Особенности организации системы мониторинга информационной безопасности от APT-атак** | Исследование системы мониторинга информационной безопасности на предмет источников данных для мониторинга. Создание технического проекта. Обучение технического персонала. Проведение тестового запуска СМИБ. | **2** | ПК-1; ПК-7 |
| | **в том числе лабораторных занятий:** | **2** | |
| | Лабораторная работа № 10.<br>Разработка сложного Playbook для расследования фишинговой атаки. Автоматизация: анализ вложения, поиск похожих писем, блокировка отправителя, опрос пользователей. | | |
| | **Самостоятельная работа обучающихся:**<br>Расчет ТСО для развертывания SOC на базе open-source решений. Учет затрат на оборудование, лицензии, персонал. | **2** | |
| **Тема 2.3 Интеллектуальный анализ событий информационной безопасности домена** | Обзор источников событий безопасности домена. Журнал Security.evtx. Журнал LocalSessionManager.evtx. | **2** | ПК-1; ПК-7 |
| | **в том числе лабораторных занятий:** | **2** | |
| | Лабораторная работа № 11.<br>Настройка панели управления для визуализации KPI SOC. Создание виджетов по топ-угрозам, источникам атак, времени реакции. | | |
| | **Самостоятельная работа обучающихся:**<br>Изучение основ языка STIX 2.x и создание простого объекта. | **2** | |
| **Тема 2.4 Интеллектуальный анализ событий информационной безопасности Linux-серверов** | Журналирование событий безопасности в Linux-подобных ОС. Выявление аномального поведения пользователей. | **2** | ПК-1; ПК-7 |
| | **в том числе лабораторных занятий:** | **2** | |
| | Лабораторная работа № 12.<br>Моделирование инцидента и его полное расследование с использованием SIEM/SOAR. Ролевая игра: аналитик SOC с использованием SIEM для сбора артефактов и SOAR для документирования. | | |
| | **Самостоятельная работа обучающихся:**<br>Разработка технического задания на доработку SIEM системы: добавление нового источника данных и создание набора правил для него. | **2** | |
| **Тема 2.5 Основы разработки информационно-** | Основные этапы разработки информационно-аналитических систем. Разработка концепции ИАС. Проектирование инфраструктуры. | **2** | ПК-1; ПК-7 |
| | **в том числе лабораторных занятий:** | **2** | |

| | | | |
|---|---|---|---|
| **аналитической системы в сфере ИБ** | Лабораторная работа № 13.<br>Сравнение детекторов: правило корреляции vs. ML-модель для одной угрозы. Реализация обоих методов и сравнение точности на синтетических данных. | | |
| | **Самостоятельная работа обучающихся:**<br>Обзор и тестирование облачных SIEM/SOAR решений. | **2** | |
| **Тема 2.6 Этапы разработки информационно-аналитической системы в сфере ИБ** | Проектирование информационной базы. Подключение возможностей готового программного обеспечения. Разработка специализированных аналитических инструментов. Внедрение и расширение ИАС. | **2** | ПК-1; ПК-7 |
| | **в том числе лабораторных занятий:** | **2** | |
| | Лабораторная работа № 14.<br>Интеграция SIEM/SOAR с системой баг-трекинга. Настройка автоматического создания тикетов на основе алертов высокой критичности. | | |
| | **Самостоятельная работа обучающихся:**<br>Анализ требований ФСТЭК к средствам мониторинга и управлению инцидентами. Сопоставление требований с возможностями современных SIEM/SOAR. | **2** | |
| **Тема 2.7 Применение моделей машинного обучения для анализа трафика** | Основные модели машинного обучения. Линейные модели, модели логистического обеспечения, регрессионные модели, кластеризованный анализ. Подготовка обучающей выборки для классификации трафика. | **2** | ПК-1; ПК-7 |
| | **в том числе лабораторных занятий:** | **2** | |
| | Лабораторная работа № 15.<br>Аудит конфигурации SIEM на соответствие базовым требованиям безопасности. Проверка настроек аутентификации, шифрования, разграничения прав доступа. | | |
| | **Самостоятельная работа обучающихся:**<br>Исследование подходов к оркестрации безопасности без использования полноценных SOAR-платформ. | **4** | |
| **Тема 2.8 Применение методов машинного обучения для анализа трафика** | Наивный байесовский классификатор. Метод опорных векторов. Метод k-ближайших соседей. Деревья принятия решений. Методы бэггинга. Методы бустинга. | **2** | ПК-1; ПК-7 |
| | **в том числе лабораторных занятий:** | **2** | |
| | Лабораторная работа № 16.<br>Проектирование архитектуры гибридного SOC. Создание схемы развертывания компонентов с учетом источников данных в облаке и локально. | | |

| | | | |
|---|---|---|---|
| | **Самостоятельная работа обучающихся:**<br>Подготовка сценария для тестирования эффективности SOC: моделирование многоэтапной атаки и оценка времени/качества реакции. | **2** | |
| **Тема 2.9 Тренды и будущее SOC: автономные SOC, AI-driven security, конфиденциальные вычисления для анализа.** | Управление проектами по внедрению инноваций в SOC. | **2** | ПК-1; ПК-7 |
| | **в том числе лабораторных занятий:** | **2** | |
| | Лабораторная работа № 17.<br>Защита итогового проекта: презентация разработанной системы мониторинга и автоматизации для заданного сценария. Обоснование архитектуры, демонстрация работы детекторов и playbook. | | |
| | **Самостоятельная работа обучающихся:**<br>Формулировка концепции для магистерской диссертации в области применения ИИ для автоматизации SOC. | **4** | |
| **Итого за 2 семестр:** | | | |
| **Лекции** | | **34** | |
| **Лабораторные работы** | | **34** | |
| **Самостоятельная работа** | | **40** | |
| **Всего:** | | **108** | |

## 3. УСЛОВИЯ РЕАЛИЗАЦИИ ПРОГРАММЫ ДИСЦИПЛИНЫ

### 3.1. Материально-техническое обеспечение

Материально-техническое обеспечение дисциплины «Системы мониторинга и управления инцидентами информационной безопасности» включает:

| Наименование помещения | Перечень основного оборудования |
|---|---|
| Лаборатория программно-аппаратных средств защиты информации | Рабочее место преподавателя;<br>Посадочные места по количеству обучающихся;<br>Автоматизированные рабочие места (ПК в сборе) с доступом в сеть Интернет;<br>Интерактивная система в составе: проектор интерактивная доска<br>Программное обеспечение:<br>Система резервного копирования Кибер Бэкап Расширенная редакция для универсальной платформы;<br>Программный комплекс по предотвращению утечек данных (DLP) Кибер Протего<br>Сетевой сканер «Ревизор Сети»;<br>TheHive, Cortex, MISP, OpenCTI;<br>AlienVault OSSIM, OSQuery |
| Аудитория для проведения занятий лекционного типа | Рабочее место преподавателя;<br>Посадочные места по количеству обучающихся;<br>Автоматизированные рабочие места (ПК в сборе) с доступом в сеть Интернет;<br>Интерактивная система в составе: проектор, интерактивная доска |
| Аудитория для самостоятельной работы обучающихся: | Автоматизированные рабочие места (ПК в сборе) с доступом в сеть Интернет;<br>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. Пелешенко, В. С. Менеджмент инцидентов информационной безопасности защищенных автоматизированных систем управления: учебное пособие / В. С. Пелешенко, С. В. Говорова, М. А. Лапина. — Ставрополь: Северо-Кавказский федеральный университет,

2017. — 86 c. — Текст: электронный // Цифровой образовательный ресурс IPR SMART: [сайт]. — URL: https://www.iprbookshop.ru/69405.html .
2. Управление инцидентами информационной безопасности на объектах информатизации с учетом нейтрализации воздействия человеческого фактора: учебное пособие / О.М. Голембиовская [и др.].. — Москва: Ай Пи Ар Медиа, 2026. — 121 с. — ISBN 978-5-4497-4323-7. — Текст: электронный // Цифровой образовательный ресурс IPR SMART: [сайт]. — URL: https://www.iprbookshop.ru/150764.html.
3. Тюгашев А. А. Интеллектуальные системы [Электронный ресурс]: учебное пособие. - Самара: СамГУПС, 2020. - 151 с. – Режим доступа: https://e.lanbook.com/book/161308

**Дополнительные источники:**

1. Абденов, А. Ж. Анализ, описание и оценка функциональных узлов SIEM-системы: учебное пособие / А. Ж. Абденов, В. А. Трушин, К. Сулайман. — Новосибирск: Новосибирский государственный технический университет, 2018. — 122 с. — ISBN 978-5-7782-3603-5. — Текст: электронный // Цифровой образовательный ресурс IPR SMART: [сайт]. — URL: *https://www.iprbookshop.ru/91179.html*.
2. Методика предотвращения инцидентов информационной безопасности за счет применения SIEM-систем: монография / О. М. Голембиовская, А. А. Рябцев, Е. В. Кондрашова [и др.]. — Москва: Ай Пи Ар Медиа, 2023. — 110 с. — ISBN 978-5-4497-2317-8. — Текст: электронный // Цифровой образовательный ресурс IPR SMART: [сайт]. — URL: *https://www.iprbookshop.ru/132568.html*.
3. Автоматизация проектирования дискретных устройств. Проектирование в среде QUARTUS PRIME. Лабораторный практикум: учебное пособие / А.П. Антонов [и др.].. — Санкт-Петербург: Санкт-Петербургский политехнический университет Петра Великого, 2018. — 138 с. — ISBN 978-5-7422-6194-0. — Текст: электронный // Цифровой образовательный ресурс IPR SMART: [сайт]. — URL: https://www.iprbookshop.ru/83325.html.
4. Ларина Т.Б. Администрирование сетей. Защита ресурсов и мониторинг: учебное пособие / Ларина Т.Б.. — Москва: Российский университет транспорта (МИИТ), 2018. — 92 с. — Текст: электронный // Цифровой образовательный ресурс IPR SMART: [сайт]. — URL: https://www.iprbookshop.ru/116018.html.
5. Программно-аппаратный комплекс для мониторинга развития геодинамических процессов в горных массивах в реальном режиме времени по параметрам электромагнитных сигналов: монография / А. А. Беспалько, А. А. Бомбизов, А. Г. Лощилов, А. П. Суржиков. — Томск: Томский политехнический университет, 2018. — 174 с. — ISBN 978-5-4387-0821-6. — Текст: электронный // Цифровой образовательный ресурс IPR SMART: [сайт]. — URL: https://www.iprbookshop.ru/98972.html

### 3.2.2. Основные электронные издания

1. Национальный институт стандартов и технологий США (NIST) — Computer Security Resource Center https://csrc.nist.gov/ (источник стандартов, включая NIST SP 800-61).
2. Федеральная служба по техническому и экспортному контролю (ФСТЭК России) https://fstec.ru/.
3. OWASP Foundation (Открытый проект безопасности веб-приложений) https://owasp.org/.

## 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** |
|---|---|---|
| - Способен разрабатывать информационно-аналитические системы в сфере информационной безопасности<br>- Руководит разработкой архитектуры комплексных систем искусственного интеллекта | *Шкала оценивания для зачета*<br>*«Отлично»* (зачет)<br>Показывает высокий уровень сформированности компетенций, т.е.:<br>- демонстрирует высокое и прочное освоение материала;<br>- исчерпывающе, четко, последовательно, грамотно и логически стройно излагает теоретический материал;<br>- правильно формирует определения;<br>- демонстрирует умения самостоятельной работы с нормативно-правовой литературой;<br>- умеет делать выводы по излагаемому материалу.<br><br>*«Хорошо» (зачет)*<br>Показывает достаточный уровень сформированности компетенций, т.е.:<br>- демонстрирует достаточно полное знание материала, основных теоретических положений;<br>- достаточно последовательно, грамотно и логически стройно излагает теоретический материал;<br>- демонстрирует умения ориентироваться в нормативно-правовой литературе;<br>- умеет делать достаточно обоснованные выводы по излагаемому материалу.<br><br>*«Удовлетворительно» (зачет)*<br>Показывает пороговый уровень сформированности компетенций, т.е.:<br>- демонстрирует общее знание изучаемого материала;<br>- испытывает затруднения при ответах на дополнительные вопросы;<br>- знает основную рекомендуемую литературу;<br>- умеет строить ответ в соответствии со структурой излагаемого материала.<br><br>*Неудовлетворительно» (незачет)*<br>Ставится в случае:<br>- незнания значительной части программного материала;<br>- невладения понятийным аппаратом дисциплины;<br>- допущения существенных ошибок при изложении учебного материала;<br>- неумения строить ответ в соответствии со структурой излагаемого вопроса;<br>- неумения делать выводы по излагаемому материалу. | Текущий контроль при проведении:<br>- письменного/устного опроса;<br>- тестирования;<br>- оценки результатов самостоятельной работы (докладов, рефератов).<br><br>Промежуточная аттестация в форме:<br>-зачета,<br>- письменных/ устных ответов,<br>- 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