Министерство науки и высшего образования РФ

Федеральное государственное бюджетное образовательное учреждение высшего образования

«Дагестанский государственный технический университет»

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ

Дисциплина Технологии обеспечения 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) 1
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 _____ Мирземагомедова М.М., к.т.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

1.1. Место дисциплины в структуре ОПОП

Дисциплина «Технологии обеспечения информационной безопасности» входит в обязательную часть учебного плана по программе магистратуры 10.04.01 Информационная безопасность, направленность «Кибербразведка и противодействие угрозам с применением технологий искусственного интеллекта»

Последующими дисциплинами являются: Управление информационной безопасностью, Технологии машинного обучения в кибербезопасности, Интеллектуальные системы информационной безопасности в промышленных системах, Системы мониторинга и управления инцидентами информационной безопасности.

1.2. Цели и задачи освоения дисциплины

Дисциплина «Технологии обеспечения 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»: формирование комплекса знаний, навыков и компетенций в области информационной безопасности и применения на практике методов и средств защиты информации на основе современных интеллектуальных технологий, средств и языков программирования..

1.3. Компетенции обучающегося, формируемые в результате освоения дисциплины

В результате освоения дисциплины «Технологии обеспечения информационной безопасности» обучающийся должен овладеть следующими компетенциями:

Таблица 1.

Код и наименование компетенции	Код и наименование индикаторов достижения компетенции
ОПК-1. Способен обосновывать требования к системе обеспечения информационной безопасности и разрабатывать проект технического задания на ее создание.	ОПК-1.2 Проектирует информационные системы с учетом технологий обеспечения информационной безопасности
	ОПК-1.3 Формирует актуальные модели угроз и нарушителей для автоматизированных информационных систем, учитывает их содержание при формировании требований технического задания, умеет разрабатывать и обосновывать критерии оценки эффективности проектируемой системы обеспечения информационной безопасности
ОПК-2. Способен разрабатывать технический проект системы (подсистемы либо компонента системы) обеспечения информационной безопасности.	ОПК-2.1 Применяет методы концептуального проектирования технологий обеспечения информационной безопасности
	ОПК-2.2 Выбирает и обосновывает преимущества методов решения задач для защиты информации компьютерных систем и сетей, а также систем обеспечения информационной безопасностью
	ОПК-2.3 Выполняет работы по защите информации при изготовлении, монтаже, наладке, испытаниях и сдаче в эксплуатацию систем и средств обеспечения информационной безопасности

2. СТРУКТУРА И СОДЕРЖАНИЕ ДИСЦИПЛИНЫ

2.1. Объем и содержание дисциплины (модуля)

Таблица 2.

Вид учебной работы	**Форма обучения**
	очная
Объем образовательной программы дисциплины (ЗЕТ/ в часах)	4/144
В том числе:	**Объем в часах**
Лекции	34
Практические занятия	-
Лабораторные занятия	34
Самостоятельная работа	40
Курсовой проект (работа), семестр	-
Промежуточная аттестация в форме экзамена, семестр	1 семестр
Часы на экзамен	36

2.2. Содержание дисциплины

Раздел дисциплины, тема лекции и вопросы	Содержание учебного материала и формы организации деятельности обучающихся	Объем в часах	Коды компетенций, формированию которых способствует элемент программы
1. Основные понятия и угрозы информационной безопасности			
Тема 1.1 Основы информационной безопасности	Определение целей и принципов защиты информации; установление, факторов, влияющих на защиту информации; основные опасности и угрозы в области информационной безопасности.	**2**	ОПК-1; ОПК-2.
	в том числе лабораторных занятий:	**2**	
	Лабораторная работа № 1. Перехват и анализ сетевых пакетов. Изучить возможности библиотеки WinPcap, изучить возможности библиотеки SharpPcap; осуществить перехват и анализ сетевых пакетов на сетевом транспортном и прикладном уровнях модели OSI.		
	Самостоятельная работа обучающихся: Основы разработки систем на языках высокого уровня.	**2**	
Тема 1.2 Классификация методов и средств защиты информации	Глубина классификации и реквизит. Классификации видов, методов и средств защиты информации. Организационная защита информации. Инженерно-техническая защита информации. Криптографическая защита информации. Представление информации в цифровом виде.	**2**	ОПК-1; ОПК-2.
	в том числе лабораторных занятий:	**2**	
	Лабораторная работа № 2. Современные симметричные криптосистемы. Изучение принципов работы симметричных криптосистем, многие из которых являются национальными или ведомственными стандартами; изучение реализаций симметричной криптографии в среде .NET Framework; программная реализация существующих симметричных криптоалгоритмов.		
	Самостоятельная работа обучающихся: Классификация методов и средств защиты информации.	**2**	
Тема 1.3 Задачи информационной безопасности	Задача обеспечения конфиденциальности. Задача обеспечения доступа. Задача обеспечения аутентификации. Обеспечение идентификации. Задача обеспечения целостности.	**2**	ОПК-1; ОПК-2.
	в том числе лабораторных занятий:	**2**	

	Лабораторная работа № 2. Современные симметричные криптосистемы. Изучение принципов работы симметричных криптосистем, многие из которых являются национальными или ведомственными стандартами; изучение реализаций симметричной криптографии в среде .NET Framework; программная реализация существующих симметричных криптоалгоритмов.		
	Самостоятельная работа обучающихся: Проектирование защищенного программного обеспечения.	**2**	
Тема 1.4 Угрозы информационной безопасности	Классификация угроз информационной безопасности. Угрозы несанкционированного доступа к данным. Угрозы нарушения целостности данных. Угрозы нарушения конфиденциальности данных.	**2**	ОПК-1; ОПК-2.
	в том числе лабораторных занятий:	**2**	
	Лабораторная работа № 3. Современные асимметричные криптосистемы. Изучение принципов работы асимметричных криптосистем; изучение реализаций асимметричной криптографии в среде .NET Framework; реализация существующих асимметричных криптоалгоритмов.		
	Самостоятельная работа обучающихся: Оценка качества разработанных защищенных программных средств системы.	**2**	
Тема 1.5 Основы государственной политики и угрозы безопасности Российской Федерации в информационной сфере	Основы законодательства в области обеспечения информационной безопасности. Правовое обеспечение информационной безопасности. Российское законодательство в области информационной безопасности. Закон «Об информации, информатизации и защите информации». Защита персональных данных. Другие законы и нормативные акты.	**2**	ОПК-1; ОПК-2.
	в том числе лабораторных занятий:	**2**	
	Лабораторная работа № 3. Современные асимметричные криптосистемы. Изучение принципов работы асимметричных криптосистем; изучение реализаций асимметричной криптографии в среде .NET Framework; реализация существующих асимметричных криптоалгоритмов.		
	Самостоятельная работа обучающихся: Обеспечение уровней безопасности.	**2**	

Тема 1.6 Понятие и виды защищаемой информации	Путь конфиденциального документа от создания до уничтожения: решение, разработка проекта, подготовка содержания, реквизитов, передача, получение, исполнение и архивация. Объект информатизации. Факторы, воздействующие на информацию. Общие положения. Защита конфиденциальной информации при ее передаче по сети.	**2**	ОПК-1; ОПК-2.
	в том числе лабораторных занятий:	**2**	
	Лабораторная работа № 4. Хэширование и электронная цифровая подпись. Изучение методов формирования дайджеста сообщения (хэш-функции) и электронной цифровой подписи (ЭЦП); изучение реализаций хэш-функций и ЭЦП в среде .NET Framework; реализация существующих хэш-функций и алгоритмов ЭЦП.		
	Самостоятельная работа обучающихся: Система защищенного электронного документооборота.	**2**	
Тема 1.7 Защита информации. Общая характеристика способов и средств защиты информации	Способы и средства защиты информации от несанкционированного доступа. Способы и средства защиты информации от вредоносного кода. Способы и средства защиты информации от межсетевого воздействия.	**2**	ОПК-1; ОПК-2.
	в том числе лабораторных занятий:	**2**	
	Лабораторная работа № 4. Хэширование и электронная цифровая подпись. Изучение методов формирования дайджеста сообщения (хэш-функции) и электронной цифровой подписи (ЭЦП); изучение реализаций хэш-функций и ЭЦП в среде .NET Framework; реализация существующих хэш-функций и алгоритмов ЭЦП.		
	Самостоятельная работа обучающихся: Способы и средства криптографической защиты информации.	**2**	
2. Методы и средства защиты информации			
Тема 2.1 Криптографические методы защиты информации	Основные понятия и термины криптографии. Краткая история развития шифров. Примеры. Основные проблемы криптографии. Оценка секретных систем. Криптостойкость. Методы криптоанализа и взлома.	**2**	ОПК-1; ОПК-2.
	в том числе лабораторных занятий:	**2**	
	Лабораторная работа № 5. Работа с системными журналами в операционной системе. Изучение методов работы с системными журналами. Отслеживание событий записи в системные журналы. Перехват системных событий. Анализ записей системных журналов.		

	Самостоятельная работа обучающихся: Парадоксы.	**2**	
Тема 2.2 Криптографические методы защиты информации. Одностороннее шифрование	Виды алгоритмов хэширования. Алгоритмы выработки имитовставки. Гаммирование. Хэш- функции.	**2**	ОПК-1; ОПК-2.
	в том числе лабораторных занятий:	**2**	
	Лабораторная работа № 5. Работа с системными журналами в операционной системе. Изучение методов работы с системными журналами. Отслеживание событий записи в системные журналы. Перехват системных событий. Анализ записей системных журналов.		
	Самостоятельная работа обучающихся: Семейство алгоритмов SHA.	**2**	
Тема 2.3 Криптографические методы защиты информации. Симметричной шифрование	Виды алгоритмов хэширования. Алгоритмы выработки имитовставки. Гаммирование. Хэш- функции. Алгоритм SHA. Симметричные шифры. Криптография с открытым ключом. Блочные и потоковые шифры.	**2**	ОПК-1; ОПК-2.
	в том числе лабораторных занятий:	**2**	
	Лабораторная работа № 6. Работа с системными журналами в операционной системе. Файловая система. Отслеживание событий изменения файловой системы (создание, удаление, переименование и изменение выбранных файлов и папок). Отслеживание событий изменения аппаратной конфигурации компьютера.		
	Самостоятельная работа обучающихся: Алгоритмы DES, AES.	**2**	
Тема 2.4 Криптографические методы защиты информации. Асимметричной шифрование	Ассиметричное шифрование, преимущества и недостатки. Понятие открытого и закрытого ключа. Алгоритм Диффи – Хеллмана. Схема алгоритма RSA.	**2**	ОПК-1; ОПК-2.
	в том числе лабораторных занятий:	**2**	
	Лабораторная работа № 6. Работа с системными журналами в операционной системе. Файловая система. Отслеживание событий изменения файловой системы (создание, удаление, переименование и изменение выбранных файлов и папок). Отслеживание событий изменения аппаратной конфигурации компьютера.		
	Самостоятельная работа обучающихся: Примеры программной реализации алгоритма RSA.	**2**	

Тема 2.5 Электронная цифровая подпись и цифровые сертификаты	Электронная цифровая подпись. Понятие о цифровой подписи. Подпись RSA. Подпись ElGamal. Подпись DSA.ЭЦП ГОСТ Р 34.10-94 и ГОСТ Р 34.10-01. Инфраструктура открытых ключей.	**2**	ОПК-1; ОПК-2.
	в том числе лабораторных занятий:	**2**	
	Лабораторная работа № 7. Удаленный доступ и управление операционной системой. Удаленный доступ к ресурсам операционной системы с использованием технологии WMI. Знакомство с утилитой командной строки wmic. Работа с протоколом удаленного доступа SSH.		
	Самостоятельная работа обучающихся: Сертификаты открытых ключей.PKI	**2**	
Тема 2.6 Обеспечение высокой доступности, туннелированные и управление	Методы и средства обеспечения высокой доступности. Проактивное управление, задание реакций, резервное копирование. Синхронное и асинхронное тиражирование. Туннелирование данных.	**2**	ОПК-1; ОПК-2.
	в том числе лабораторных занятий:	**2**	
	Лабораторная работа № 7. Удаленный доступ и управление операционной системой. Удаленный доступ к ресурсам операционной системы с использованием технологии WMI. Знакомство с утилитой командной строки wmic. Работа с протоколом удаленного доступа SSH.		
	Самостоятельная работа обучающихся: Мониторинг и контроль.	**2**	
Тема 2.7 Практические аспекты криптографии	Способы взлома и кражи данных в сетях. Защита протокола WiFi. Протокол HTTPs. Виртуальные персональные сетевые каналы VPS. Схема работы протокола TOR.	**2**	ОПК-1; ОПК-2.
	в том числе лабораторных занятий:	**2**	
	Лабораторная работа № 8. Управление политиками безопасности. Исследование методов контроля доступа к ресурсам операционной системы. Обеспечение безопасности доступа кода. Управление политиками безопасности.		
	Самостоятельная работа обучающихся: Сетевой протокол прикладного уровня, позволяющий производить удалённое управление SSH.	**2**	
Тема 2.8 Методы организации безопасного доступа	Схемы идентификации и аутентификации. Одно- и многофакторная аутентификация. Система разграничения доступа к информации в компьютерной системе. Концепция построения систем разграничения доступа.	**2**	ОПК-1; ОПК-2.

	в том числе лабораторных занятий:	**2**	
	Лабораторная работа № 8. Управление политиками безопасности. Исследование методов контроля доступа к ресурсам операционной системы. Обеспечение безопасности доступа кода. Управление политиками безопасности.		
	Самостоятельная работа обучающихся: Средства и методы ограничения доступа к файлам.	**4**	
Тема 2.9 Программно-аппаратные средства защиты информации	Аппаратные и программно-аппаратные средства криптозащиты данных. Использование дополнительных плат расширения. Методы «водяных знаков» и методы «отпечатков пальцев».	**2**	ОПК-1; ОПК-2.
	в том числе лабораторных занятий:	**2**	
	Лабораторная работа № 9. Практическая реализация распределения ключей. Безопасное распределение ключей. Алгоритм Диффи-Хеллмана.		
	Самостоятельная работа обучающихся: Защита программ от несанкционированного копирования.	**4**	
Тема 2.10 Классификация вирусов. Применение антивирусных программ	Классификация вирусных программ. Основные признаки заражения от вредоносных программ. Методы заражения. История антивирусных программ, сведения о надежности и механизмах работы современных антивирусных программ.	**2**	ОПК-1; ОПК-2.
	в том числе лабораторных занятий:	**2**	
	Лабораторная работа № 9. Практическая реализация распределения ключей. Безопасное распределение ключей. Алгоритм Диффи-Хеллмана.		
	Самостоятельная работа обучающихся: Основные моменты использования современных антивирусных программ.	**4**	
Итого за 1 семестр:			
Лекции		**34**	
Лабораторные работы		**34**	
Самостоятельная работа		**40**	
Промежуточная аттестация в форме экзамена		**36**	
Всего:		**144**	

3. УСЛОВИЯ РЕАЛИЗАЦИИ ПРОГРАММЫ ДИСЦИПЛИНЫ

3.1. Материально-техническое обеспечение

Материально-техническое обеспечение дисциплины «Технологии обеспечения информационной безопасности» включает:

Наименование помещения	Перечень основного оборудования
Лаборатория программно-аппаратных средств 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»; Программно-аппаратный комплекс «Соболь»; «ФИКС» - программа фиксации и контроля исходного состояния программного комплекса; TERRIER» - программа поиска и гарантированного уничтожения информации на дисках; «Ревизор 1 XP» - средство создания модели системы разграничения доступа; «Ревизор 2 XP» - программа контроля полномочий доступа к информационным ресурсам; Сетевой сканер «Ревизор Сети»; «ПИК-Lite» - программа подсчета контрольных сумм; Dallas Lock - система защиты информации от несанкционированного доступа в процессе хранения и обработки; Система резервного копирования Кибер Бэкап Расширенная редакция для универсальной платформы; Программный комплекс по предотвращению утечек данных (DLP) Кибер Протего Компьютер RAMEC GALE - корпоративная рабочая станция; Электронный ключ GUARDANT ID; Электронный ключ Rutoken; Средство контроля эффективности применения СЗИ; Программа фиксации и контроля исходного состояния программного комплекса, «Фикс-Unix 1.0»; Программа расчета контрольных сумм «gostum» из состава ОС специального назначения «Astra Linux SE»; Средство контроля эффективности применения СЗИ; Программа фиксации и контроля исходного состояния программного комплекса, «Фикс»; Средство создания модели системы разграничения доступа, «Ревизор 1XP»; Средство контроля защищенности информации от НСД в АС; Программа контроля полномочий доступа к информационным ресурсам, «Ревизор 2XP»; Средство защиты и контроля эффективности применения СЗИ; Программа поиска и гарантированного уничтожения информации на дисках «Terrier»; Средство сбора информации о программном и аппаратном обеспечении в АС «Агент

	инвентаризации»; СЗИ НСД Аккорд-АМДЗ. Базовый набор функций, шина PCI-express, прошивка с поддержкой UEFI (арт.P79UGX); Съемник информации с контактным устройством DS-USB (арт. 920500); Право на использование СПО ПАК СЗИ НСД «Аккорд-Win64»; Право на использование СПО «Аккорд-X»; Служебный носитель «Секрет Особого Назначения» криптографический с быстрым процессором, 32Гб (арт. 620520)
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. Пестов, И. Е. Технологии обеспечения информационной безопасности больших данных: учебное пособие / И. Е. Пестов, Л. А. Виткова, С. Н. Шемякин. — Санкт-Петербург: СПбГУТ им. М.А. Бонч-Бруевича, 2025. — 94 с. — ISBN 978-5-89160-356-1. — Текст: электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/508652.
2. Технологии обеспечения информационной безопасности больших данных в компьютерных сетях. Информационная безопасность в системах обработки данных на примере Hadoop и Spark: учебно-методическое пособие / составители А. В. Осин, К. А. Хализев. — Москва: МТУСИ, 2025. — 18 с. — Текст: электронный // Лань: электронно-библиотечная система. — URL: https://e.lanbook.com/book/501212.
3. Импортозамещающие технологии обеспечения информационной безопасности и защиты данных: учебное пособие / Д. А. Короченцев, Л. В. Черкесова, Е. А. Ревякина [и др.]. — Ростов-на-Дону: Донской ГТУ, 2021. — 335 с. — ISBN 978-5-7890-1893-4. — Текст: электронный // Лань: электронно-библиотечная система. — URL: https://e.lanbook.com/book/237782.

Дополнительные источники:

1. Схиртладзе, А. Г. Информатика, современные информационные технологии: учебник / А. Г. Схиртладзе, В. П. Мельников, В. Б. Моисеев. — Пенза: ПензГТУ, 2015. — 548 с. —

Текст: электронный // Лань: электронно-библиотечная система. — URL: https://e.lanbook.com/book/63098.
2. Раханов, К. Я. Обеспечение конфиденциальности информации в сети Интернет: учебное пособие / К. Я. Раханов, Н. А. Раханова. — Новополоцк: ПГУ им. Евфросинии Полоцкой, 2021. — 192 с. — ISBN 978-985-531-723-5. — Текст: электронный // Лань: электронно-библиотечная система. — URL: https://e.lanbook.com/book/366821.
3. Поздняк, И. С. Управление информационной безопасностью: учебное пособие / И. С. Поздняк, И. С. Макаров. — Самара: ПГУТИ, 2023. — 104 с. — Текст: электронный // Лань: электронно-библиотечная система. — URL: https://e.lanbook.com/book/463619.

3.2.2. Основные электронные издания

1. Портал «Информационная безопасность»: новости, публикации, инновации – Архив изданий по информационной безопасности https://www.itsec.ru/articles2/allpubliks
2. Уязвимости, обзоры, аналитика и многое другое – Портал информационной безопасности — Securitylab.ru
3. Отслеживание тенденций, аналитика, информирование о наиболее значимых событиях - BugTraq.Ru
4. Backtrack Linux LiveCD и образ для виртуальной машины Сайт проекта Linux для анализа компьютерной безопасности
5. Блоги и статьи специалистов по ИБ InformIT
6. Электронная библиотека - Режим доступа: http://elibrary.ru
7. Электронная библиотечная система «КнигаФонд» − http://www.knigafund.ru/
8. Электронная библиотечная система издательства «Лань» − http://e.lanbook.com/

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**
- Проектирует информационные системы с учетом технологий обеспечения информационной безопасности - Формирует актуальные модели угроз и нарушителей для автоматизированных информационных систем, учитывает их содержание при формировании требований технического задания, умеет разрабатывать и обосновывать критерии оценки эффективности проектируемой системы обеспечения информационной безопасности - Применяет методы концептуального проектирования технологий обеспечения информационной безопасности - Выбирает и обосновывает преимущества методов решения задач для защиты информации компьютерных систем и сетей, а также систем обеспечения информационной безопасностью - Выполняет работы по защите информации при изготовлении, монтаже, наладке, испытаниях и сдаче в эксплуатацию систем и средств обеспечения информационной безопасности	*Шкала оценивания для экзамена* *«Отлично»* Показывает высокий уровень сформированности компетенций, т.е.: - 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. *«Хорошо»* Показывает достаточный уровень сформированности компетенций, т.е.: - 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. *«Удовлетворительно»* Показывает пороговый уровень сформированности компетенций, т.е.: - 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. *Неудовлетворительно»* Ставится в случае: - 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.	Текущий контроль при проведении: - письменного/устного опроса; - тестирования; - оценки результатов самостоятельной работы (докладов, рефератов). Промежуточная аттестация в форме: -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