МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ
федеральное государственное бюджетное образовательное учреждение высшего образования «Казанский национальный исследовательский технический университет им. А.Н. Туполева-КАИ»
Лениногорский филиал

УТВЕРЖДАЮ
Директор ЛФ КНИТУ-КАИ
__________ Р.А. Шамсутдинов
«_24_»__06__________ 2021 г.

РАБОЧАЯ ПРОГРАММА

дисциплины (модуля)

Б1.О.16 Защита информации
(индекс и наименование дисциплины по учебному плану)

Квалификация: *бакалавр*

Форма обучения: *очная, заочная*

Направление подготовки: ***09.03.02 Информационные системы и технологии***

Направленность (профиль): ***Информационные системы и технологии***

Лениногорск 2021

Рабочая программа дисциплины (модуля) разработана в соответствии с требованиями федерального государственного образовательного стандарта высшего образования по направлению подготовки 09.03.02 Информационные системы и технологии, утвержденного приказом Министерства образования и науки Российской Федерации от 19 сентября 2017г. № 926.

Разработчик(и):
Сагдатуллин А.М., к.т.н
(ФИО, ученая степень, ученое звание) *(подпись)*

Лямов Ю.О., старший преподаватель
(ФИО, ученая степень, ученое звание) *(подпись)*

Рабочая программа утверждена на заседании кафедры МиИТ от «22» июня 2021г., протокол № 11-1.

/Заведующий кафедрой МиИТ
Думлер Е.Б., к.т.н.
(ФИО, ученая степень, ученое звание) *(подпись)*

Рабочая программа дисциплины (модуля):	Наименование Подразделения	Дата	№ протокола	Подпись
ОДОБРЕНА	на заседании кафедры МиИТ	22.06.2021	11-1	Руководитель ОП А.М. Сагдатуллин
ОДОБРЕНА	Учебно-методическая комиссия ЛФ КНИТУ-КАИ	24.06.2021	10	Председатель УМК З.И.Аскарова
СОГЛАСОВАНА	Научно-техническая библиотека	24.06.2021		Библиотекарь А.Г. Страшнова

1 ИСХОДНЫЕ ДАННЫЕ И КОНЕЧНЫЙ РЕЗУЛЬТАТ ИЗУЧЕНИЯ ДИСЦИПЛИНЫ (МОДУЛЯ)

1.1 Цель изучения дисциплины (модуля)

Целью изучения дисциплины является: изучение основных принципов, методов и средств защиты информации в процессе ее обработки, передачи и хранения с использованием компьютерных средств в информационных системах.

1.2 Задачи дисциплины (модуля)

– освоение защиты информации как систематической научно-практической деятельности, носящей прикладной характер;

– знание базовых теоретических понятий, лежащих в основе процесса защиты информации;

– усвоение методов и способов защиты информации.

1.3 Место дисциплины (модуля) в структуре ОП ВО

Дисциплина относится к обязательной части Блока 1. Дисциплины (модули) образовательной программы.

1.4 Объем дисциплины (модуля) и виды учебной работы

Объем дисциплины (модуля) в зачетных единицах с указанием количества академических часов, выделенных на контактную работу обучающихся с преподавателем (по видам учебных занятий) и на самостоятельную работу обучающихся представлены в таблице 1.1

Таблица 1.1а

Объем дисциплины (модуля) для очной формы обучения

Семестр	Общая трудоемкость дисциплины (модуля), в ЗЕ/час	*Виды учебной работы, в т.ч., проводимые с использованием ЭО и ДОТ*											
		Контактная работа обучающихся с преподавателем по видам учебной работы (аудиторная работа)							***Самостоятельная работа обучающегося (внеаудиторная работа)***				
		Лекции/ в т.ч. в форме практической подготовки	Лабораторные работы/ в т.ч. в форме практической подготовки	Практические занятия/ в т.ч. в форме практической подготовки	Курсовая работа (консультация, защита)	Курсовой проект (консультации, защита)	Консультации перед экзаменом	Контактная работа на промежуточной аттестации	Курсовая работа (подготовка)/ в т.ч. в форме практической	Курсовой проект (подготовка)/ в т.ч. в форме практической	Проработка учебного материала (самоподготовка)/ в т.ч. в форме практической подготовки	Подготовка к промежуточной аттестации	Форма промежуточной аттестации
8	3 ЗЕ/108	16	16/16	-	-	-	-	0,3	-	-	75,7	-	Зачет
Итого	**3 ЗЕ/108**	**16**	**16/16**	**-**	**-**	**-**	**-**	**0,3**	**-**	**-**	**75,7**	**-**	

Таблица 1.1б

Объем дисциплины (модуля) для заочной формы обучения

Семестр	Общая трудоемкость дисциплины (модуля), в ЗЕ/час	*Виды учебной работы, в т.ч., проводимые с использованием ЭО и ДОТ*											
		Контактная работа обучающихся с преподавателем по видам учебной работы (аудиторная работа)							***Самостоятельная работа обучающегося (внеаудиторная работа)***				
		Лекции/ в т.ч. в форме практической подготовки	Лабораторные работы/ в т.ч. в форме практической подготовки	Практические занятия/ в т.ч. в форме практической подготовки	Курсовая работа (консультация, защита)	Курсовой проект (консультации, защита)	Консультации перед экзаменом	Контактная работа на промежуточной аттестации	Курсовая работа (подготовка)/ в т.ч. в форме практической	Курсовой проект (подготовка)/ в т.ч. в форме практической	Проработка учебного материала (самоподготовка)/ в т.ч. в форме практической подготовки	Подготовка к промежуточной аттестации	Форма промежуточной аттестации
10	3 ЗЕ/108	4	8/8	-	-	-	-	0,3	-	-	92	3,7	Зачет
Итого	**3 ЗЕ/108**	**4**	**8/8**	**-**	**-**	**-**	**-**	**0,3**			**92**	**3,7**	

1.5 Перечень планируемых результатов обучения по дисциплине (модулю)

Процесс изучения дисциплины направлен на формирование компетенций, представленных в таблице 1.2.

Таблица 1.2

Формируемые компетенции

Код компетенции	Наименование компетенции	Индикаторы достижения компетенций	Планируемые результаты обучения
ОПК-2	Способен понимать принципы работы современных информационных технологий и программных средств, в том числе отечественного производства, и использовать их при решении задач профессиональной деятельности	ИД-1$_{ОПК-2}$ - Обоснованно выбирает современные информационные технологии, инструментальные среды и программные средства, в том числе отечественного производства; ИД-2$_{ОПК-2}$ - Применяет/использует современные информационные технологии и программные средства, в том числе отечественного производства, при решении задач.	**Знает** виды программного обеспечения для защиты данных, в том числе отечественного производства; **Умеет** выбирать и применять программные средства для защиты информации и разграничения доступа; **Владеет** навыками работы с программными с программными средствами для защиты данных, поиска и устранения вредоносных программ, восстановления поврежденных или утраченных данных.

ОПК-3	Способен решать стандартные задачи профессиональной деятельности на основе информационной и библиографической культуры с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности	ИД-1$_{ОПК-3}$ – Применяет актуальные информационные и библиографические источники при решении стандартных задач профессиональной деятельности; ИД-2$_{ОПК-3}$ – Применяет требования информационной безопасности при использовании информационно-коммуникационных технологий.	**Знает** особенности вредоносных программ, принципы их работы и виды ответственности за их незаконное применение, способы защиты информации от несанкционированного доступа; **Умеет** определять типы вредоносных программ и последствия их работы, выполнять шифрование данных для защиты от несанкционированного доступа; **Владеет** навыками устранения вредоносных программ с помощью программных средств защиты, шифрования и дешифрования информации различными методами.

2 СОДЕРЖАНИЕ ДИСЦИПЛИНЫ (МОДУЛЯ)

2.1 Структура дисциплины (модуля)

Содержание дисциплины (модуля), структурированное по темам (разделам), с указанием отведенного на них количества академических часов и видов учебных занятий приведены в таблице 2.1.

Таблица 2.1

Разделы дисциплины (модуля) и виды занятий

Наименование тем (разделов) дисциплины (модуля)	Всего (час)	Контактная работа обучающихся с преподавателем по видам учебных занятий (в час)				Самостоятельная работа (проработка учебного материала), выполнение курсовой работы /проекта, подготовка и ПА, самоподготовка.
		Лекции	Лабораторные работы	Практические занятия	КР, КП, ПА, консультация	
8 семестр						
1 Основные понятия и определения. Концептуальные основы защиты информации	22	3	4			15
2 Организационно-правовые аспекты защиты информации. Политика безопасности и управление рисками	18,7	3				15,7
3 Стандартизация в сфере ИТ-безопасности	22	3	4			15
4 Математические методы и модели в задачах защиты информации	23	4	4			15
5 Многоуровневая защита информации в компьютерных системах и сетях	22	3	4			15
Промежуточная аттестация (зачет)	0,3				0,3	
Итого за семестр	**108**	**16**	**16**		**0,3**	**75,7**

2.2 Содержание разделов дисциплины (модуля)

1. Основные понятия и определения. Концептуальные основы защиты информации.

Становление и развитие понятия «информационная безопасность». Современные подходы к определению понятия. Сущность информационной безопасности, характеристика ее составляющих. Объекты информационной безопасности. Связь информационной безопасности с информатизацией

общества. Структура информационной безопасности. Определение понятия “информационная безопасность”.

Значение информационной безопасности для субъектов информационных отношений. Связь между информационной безопасностью и безопасностью информации. Понятие и современная концепция национальной безопасности. Место информационной безопасности в системе национальной безопасности.

2. Организационно-правовые аспекты защиты информации. Политика безопасности и управление рисками.

Современная концепция информационной безопасности Российской Федерации. Понятие и назначение Доктрины информационной безопасности. Интересы личности, общества и государства в информационной сфере. Составляющие национальных интересов в информационной сфере, пути их достижения. Виды и состав угроз информационной безопасности. Состояние информационной безопасности Российской Федерации и основные задачи по их обеспечению. Принципы обеспечения информационной безопасности. Общие методы обеспечения информационной безопасности. Особенности обеспечения информационной безопасности в различных сферах общественной жизни. Основные положения государственной политики обеспечения информационной безопасности, мероприятия по их реализации. Организационная основа системы обеспечения информационной безопасности.

3. Стандартизация в сфере ИТ-безопасности.

Правовые основы стандартизации и сертификации в РФ и зарубежных странах. Гармонизация российской системы стандартизации и сертификации с европейскими и международными правилами. Закон о техническом регулировании. Основные понятия. Закон о техническом регулировании. Понятия технических регламентов и стандартизации.

Организационная структура технического комитета ИСО 176, модель описания системы качества в стандартах ИСО 9001 и 9004 и модели функционирования системы менеджмента качества (СМК), основанной на процессном подходе.

Схемы сертификации, инфраструктура сертификации ИКТ в образовании, сертификация в жизненном цикле программной продукции и результаты экспертной оценки.

4. Математические методы и модели в задачах защиты информации.

Основные понятия криптографии. Краткая история развития криптологии. Основные понятия и определения. Подстановочные и перестановочные шифры. Шифры Цезаря, Виженера, Вернома.

Исследования Шеннона в области криптографии. Нераскрываемость шифра Вернома. Симметричные системы шифрования. Основные понятия и

определения. Классификация симметричных систем шифрования: поточные шифры, блочные шифры. Блочные шифры. Сеть Фейштеля. Алгоритм TEA. Алгоритм DES. Алгоритм ГОСТ 28147-89. Сравнение алгоритмов DES и ГОСТ 28147-89. Модификация алгоритма DES: тройной DES с двумя и тремя ключами. Алгоритм AES. Режимы выполнения алгоритмов шифрования: EBC, CBC, CFB и OFB.

Потоковые шифры. Алгоритм RC4. Математические основы криптографических методов. Основные понятия и определения теории информации. Основные теоремы теории чисел (арифметика вычетов, малая теорема Ферма, теорема Эйлера, разложение числа на простые сомножители). Наибольший общий делитель. Алгоритм Евклида. Обобщенный алгоритм Евклида. Возведение в степень по модулю. Дискретные логарифмы в конечном поле. Понятия однонаправленной функции и однонаправленной функции с лазейкой. Элементы теории сложности проблем.

Классы сложности проблем.

5. Многоуровневая защита информации в компьютерных системах и сетях.

Принципы многоуровневой защиты информации. Обеспечение безопасности операционных систем. Протоколы защищенных каналов.

Технологии межсетевого экранирования. Технологии виртуальных защищенных сетей VPN. Защита удаленного доступа. Технологии обнаружения и предотвращения вторжений. Технологи защиты от вредоносных программ и спама.

2.3 Курсовая работа (курсовой проект)

Не предусмотрено учебным планом.

3 ОЦЕНОЧНЫЕ МАТЕРИАЛЫ И МЕТОДИЧЕСКИЕ РЕКОМЕНДАЦИИ ПО ОСВОЕНИЮ ДИСЦИПЛИНЫ (МОДУЛЯ)

3.1 Содержание оценочных материалов и их соответствие запланированным результатам обучения

Текущий контроль успеваемости обеспечивает оценивание хода освоения дисциплины (модуля). Перечень оценочных средств текущего контроля представлен в таблице 3.1.

Таблица 3.1

Оценочные средства текущего контроля

Виды учебных занятий	Наименование оценочного средства текущего контроля	Код и индикатор достижения компетенции
Лекции	Тестовые задания текущего контроля, вопросы на занятиях	ИД-1$_{ОПК-2}$, ИД-1$_{ОПК-3}$
Лабораторные работы	Отчет по лабораторным работам	ИД-2$_{ОПК-2}$, ИД-2$_{ОПК-3}$, ИД-3$_{ОПК-2}$, ИД-3$_{ОПК-3}$
Самостоятельная работа	Вопросы для самоподготовки, тестирование	ИД-1$_{ОПК-2}$, ИД-1$_{ОПК-3}$, ИД-2$_{ОПК-2}$, ИД-2$_{ОПК-3}$, ИД-3$_{ОПК-2}$, ИД-3$_{ОПК-3}$

Типовые контрольные задания или иные материалы, необходимые для оценки знаний, умений, навыков и (или) опыта деятельности, характеризующие процесс формирования компетенций в ходе освоения образовательной программы.

Примеры тестовых заданий текущего контроля:

1 Вредоносные программы - это

- Шпионские программы
- Программы, наносящие вред данным и программам, находящимся на компьютере
- Антивирусные программы
- Программы, наносящие вред пользователю, работающему на зараженном компьютере
- Троянские утилиты и сетевые черви

2 Вид угрозы действия, направленного на несанкционированное использование информационных ресурсов, не оказывающего при этом влияния на её функционирование – … угроза

- Активная
- Умышленная
- Пассивная

3 Сервисы безопасности это

- Обеспечение безопасного восстановления
- Инверсия паролей
- Контроль целостности
- Регулирование конфликтов
- Шифрование
- Кэширование записей
- Экранирование

4 Антивирусная программа – специализированная программа для обнаружения компьютерных вирусов, нежелательных программ вообще и восстановления зараженных такими программами файлов, а также для профилактики – предотвращения заражения файлов или операционной системы вредоносным кодом.

- Antivirus Kaspersky
- DrWeb
- Avast
- Nod 32

Примеры тем устных опросов на занятиях:

1. Виды шифров и принципы их работы
2. Устройство вредоносных программ и особенности их работы
3. Методы борьбы с вредоносными программами

Вопросы к лабораторным работам приведены в методических указаниях по выполнению соответствующих лабораторных работ.

Примеры вопросов для самоподготовки:

1. Принцип работы алгоритма RSA
2. Принцип работы алгоритма DES
3. Принцип работы алгоритма RC4

Полный комплект материалов (текущего и промежуточного контроля), необходимых для оценивания результатов освоения дисциплины (модуля), хранится на кафедре-разработчике в бумажном или электронном виде.

3.2 Содержание оценочных материалов промежуточной аттестации

Промежуточная аттестация обеспечивает оценивание промежуточных результатов обучения по дисциплине (модулю).

Для оценки степени сформированности компетенций используются оценочные материалы, включающие тестовые задания и контрольные (экзаменационные) вопросы.

Тестовые задания представляют собой совокупность тестовых вопросов текущего контроля по числу текущих аттестаций.

Примеры вопросов к зачету:

1. Система аутентификации по схеме «запрос-ответ»
2. Обзор современных протоколов аутентификации.
3. Обзор современных защищенных сетевых протоколов.
4. Угрозы безопасности в глобальных сетях
5. Межсетевые экраны: назначение, основные функции, состав

3.3 Оценка успеваемости обучающихся

Текущий контроль успеваемости и промежуточная аттестация по дисциплине (модулю) осуществляется в соответствии с балльно-рейтинговой системой по 100-балльной шкале. Балльные оценки для контрольных мероприятий представлены в таблице 3.2. Пересчет суммы баллов в традиционную оценку представлен в таблице 3.3.

Таблица 3.2

Бальные оценки для контрольных мероприятий

Наименование контрольного мероприятия	Максимальный балл на первую аттестацию	Максимальный балл за вторую аттестацию	Максимальный балл за третью аттестацию	Всего за семестр
8 семестр				
Тестирование	5	5	5	15
Устный опрос на занятии	1	2	2	5
Отчет по лабораторной работе	10	10	10	10
Итого (максимум за период)	**16**	**17**	**17**	**50**
Зачет				**50**
Итого				**100**

Таблица 3.3

Шкала оценки на промежуточной аттестации

Выражение в баллах	Словесное выражение при форме промежуточной аттестации - зачет	Словесное выражение при форме промежуточной аттестации - экзамен
от 86 до 100	Зачтено	Отлично
от 71 до 85	Зачтено	Хорошо
от 51 до 70	Зачтено	Удовлетворительно
до 51	Не зачтено	Не удовлетворительно

4 ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ (МОДУЛЯ)

4.1 Учебно-методическое и информационное обеспечение дисциплины (модуля)

4.1.1.Основная литература:

1. Щеглов, А. Ю. Защита информации: основы теории [Электронный ресурс]: учебник для вузов / А. Ю. Щеглов, К. А. Щеглов. — М.: Издательство Юрайт, 2021. — 309 с. — (Высшее образование). — Текст: электронный // ЭБС Юрайт [сайт]. — URL: https://urait.ru/bcode/469866

2. Баранова, Е. К. Информационная безопасность и защита информации [Электронный ресурс]: учебное пособие / Е.К. Баранова, А.В. Бабаш. — 4-е изд., перераб. и доп. — М.: РИОР: ИНФРА-М, 2021. — 336 с. — (Высшее образование). — Текст: электронный. – URL: https://znanium.com/catalog/product/1189326

3. Тумбинская, М. В. Защита информации на предприятии [Электронный ресурс]: учебное пособие / М. В. Тумбинская, М. В. Петровский. — СПб: Лань, 2020. — 184 с. — Текст: электронный // Лань: электронно-библиотечная система. — URL: https://e.lanbook.com/book/130184

4.1.2. Дополнительная литература:

1. Внуков, А. А. Защита информации [Электронный ресурс]: учебное пособие для вузов / А. А. Внуков. — 3-е изд., перераб. и доп. — М.: Издательство Юрайт, 2021. — 161 с. — (Высшее образование). — Текст: электронный // ЭБС Юрайт [сайт]. — URL: https://urait.ru/bcode/470131

2. Краковский, Ю. М. Методы защиты информации [Электронный ресурс]: учебное пособие для вузов / Ю. М. Краковский. — 3-е изд., перераб. — СПб: Лань, 2021. — 236 с. — Текст: электронный // Лань: электронно-библиотечная система. — URL: https://e.lanbook.com/book/156401

3. Хорев, П. Б. Программно-аппаратная защита информации [Электронный ресурс]: учебное пособие / П.Б. Хорев. — 3-е изд., испр. и доп. — М.: ИНФРА-М, 2021. — 327 с. — (Высшее образование: Бакалавриат). — Текст: электронный. - URL: https://znanium.com/catalog/product/1189342

4. Шаньгин, В. Ф. Комплексная защита информации в корпоративных системах [Электронный ресурс]: учебное пособие / В. Ф. Шаньгин. — М.: ФОРУМ: ИНФРА-М, 2022. — 592 с. — (Высшее образование: Бакалавриат). - Текст: электронный. - URL: https://znanium.com/catalog/product/1843022

4.1.3 Методические материалы

1. Методические указания к выполнению лабораторных работ
2. Методические указания по самостоятельной работе

3. Лямов Ю.О. «Защита информации» [Электронный ресурс]: курс дистанционного обучения по направлению подготовки бакалавров 09.03.02 «Информационные системы и технологии» / КНИТУ-КАИ (Лениногорский филиал), Лениногорск, 2020 – Доступ по логину и паролю. URL: https://bb.kai.ru:8443/webapps/blackboard/execute/content/blankPage?cmd=view&content_id=_350724_1&course_id=_14923_1

Идентификатор курса 20_Leninogorsk_MiIT_yuolyamov_ZI.

4.1.4 Перечень информационных технологий и электронных ресурсов, используемых при осуществлении образовательного процесса по дисциплине (модулю)

Организовано взаимодействие обучающегося и преподавателя с использованием электронной информационно-образовательной среды КНИТУ-КАИ.

1. Лямов Ю.О. «Защита информации» [Электронный ресурс]: курс дистанционного обучения по направлению подготовки бакалавров 09.03.02 «Информационные системы и технологии» / КНИТУ-КАИ (Лениногорский филиал), Лениногорск, 2020 – Доступ по логину и паролю. URL: https://bb.kai.ru:8443/webapps/blackboard/execute/content/blankPage?cmd=view&content_id=_350724_1&course_id=_14923_1

Идентификатор курса 20_Leninogorsk_MiIT_yuolyamov_ZI.

4.1.5 Перечень ресурсов информационно-телекоммуникационной сети «Интернет», профессиональных баз данных, информационно-справочных систем, используемых при осуществлении образовательного процесса по дисциплине (модулю)

1. Электронно-библиотечная система учебной и научной литературы «Лань». URL:https://e.lanbook.com/.
2. Электронно-библиотечная система учебной и научной литературы «Znanium/com». URL: https://znanium.com/
3. Электронно-библиотечная система учебной и научной литературы «Юрайт». URL: https://urait.ru/catalog/full
4. Научно-техническая библиотека КНИТУ-КАИ им. Н.Г. Четаева. URL: http://elibs.kai.ru/
5. UDEMY – Курсы по информационной безопасности, URL: https://www.udemy.com/ru/courses/it-and-software/network-and-security
6. Справочная правовая система «КонсультантПлюс».

4.2 Материально-техническое обеспечение дисциплины (модуля) и требуемое программное обеспечение

Описание материально-технической базы и программного обеспечения, необходимого для осуществления образовательного процесса по дисциплине (модулю) приведено соответственно в таблицах 4.1 и 4.2.

Таблица 4.1

Материально-техническое обеспечение дисциплины (модуля)

Наименование вида учебных занятий	Наименование учебной аудитории, специализированной лаборатории	Перечень необходимого оборудования и технических средств обучения
Лекционные занятия	Учебная аудитория для проведения занятий лекционного типа (Л. 302)	- мультимедийный проектор; - ноутбук; - настенный экран; - акустические колонки; - учебные столы, стулья; - доска; - стол преподавателя.
Лабораторные занятия	Компьютерная аудитория (Л. 201)	- учебные столы, стулья; - доска; - стол преподавателя; - компьютерные столы, стулья; - персональные компьютеры; - локальная вычислительная сеть; - ЖК мониторы 23”; - доска интерактивная; - мультимедиа-проектор.
Самостоятельная работа	Помещение для самостоятельной работы студента (Л. 112)	- персональный компьютер; - ЖК монитор 19”; - столы компьютерные; - учебные столы, стулья.

Таблица 4.2

Лицензионное и свободно распространяемое программное обеспечение, в том числе отечественного производства, используемое при осуществлении образовательного процесса по дисциплине (модулю)

№ п/п	Наименование программного обеспечения	Производитель	Способ распространения (лицензионное или свободно распространяемое)
1	– Kleopatra – программное обеспечение для шифрования		Свободно распространяемое
2	Microsoft Windows 7 Professional Russian	Microsoft, США	Лицензионное
3	Microsoft Office Professional Plus 2010 Russian	Microsoft, США	Лицензионное
4	Антивирусная программа Kaspersky Endpoint Security 8 for Windows	Лаборатория Касперского, Россия	Лицензионное
5	– Microsoft Visual Studio 2019	Microsoft, США	Лицензионное

5 ОСОБЕННОСТИ РЕАЛИЗАЦИИ ДИСЦИПЛИНЫ (МОДУЛЯ) ДЛЯ ЛИЦ С ОГРАНИЧЕННЫМИ ВОЗМОЖНОСТЯМИ ЗДОРОВЬЯ И ИНВАЛИДОВ

Обучение по дисциплине (модулю) обучающихся с ограниченными возможностями здоровья и инвалидов осуществляется с учетом особенностей психофизического развития, индивидуальных возможностей и состояния здоровья таких обучающихся.

Обучение лиц с ограниченными возможностями здоровья и инвалидов организуется как совместно с другими обучающимися, так и в отдельных группах.

Для лиц с ограниченными возможностями здоровья и инвалидов предусмотрены дополнительные оценочные материалы, перечень которых указан в таблице 5.1.

Таблица 5.1

Дополнительные материалы оценивания для лиц с ограниченными возможностями здоровья и инвалидов

Категории обучающихся	Виды дополнительных оценочных материалов	Формы контроля и оценки результатов обучения
С нарушениями слуха	Тесты, контрольные работы, письменные самостоятельные работы, вопросы к зачету (экзамену)	Преимущественно письменная проверка
С нарушениями зрения	Устный опрос по терминам, собеседование по вопросам к зачету (экзамену)	Преимущественно устная проверка (индивидуально)
С нарушениями опорно-двигательного аппарата	Решение дистанционных тестов, контрольные работы, письменные самостоятельные работы, вопросы к зачету (экзамену)	Преимущественно дистанционными методами

Для лиц с ограниченными возможностями здоровья и инвалидов предусматривается доступная форма предоставления заданий оценочных средств, например:

– в печатной форме;

– в печатной форме с увеличенным шрифтом;

– в форме электронного документа;

– методом чтения ассистентом задания вслух.

Лицам с ограниченными возможностями здоровья и инвалидам увеличивается время на подготовку ответов на контрольные вопросы. Для таких обучающихся предусматривается доступная форма предоставления ответов на задания, а именно:

– письменно на бумаге;

– набор ответов на компьютере;

– набор ответов с использованием услуг ассистента;

– представление ответов устно.

При необходимости для лиц с ограниченными возможностями здоровья и инвалидов процедура оценивания результатов обучения может проводиться в несколько этапов.

Учебно-методические материалы для самостоятельной и аудиторной работы обучающихся из числа лиц с ограниченными возможностями здоровья и инвалидов предоставляются в формах, адаптированных к ограничениям их здоровья и восприятия информации.

Освоение дисциплины (модуля) лицами с ограниченными возможностями здоровья и инвалидами осуществляется с использованием средств обучения общего и специального назначения.

ЛИСТ РЕГИСТРАЦИИ ИЗМЕНЕНИЙ

Изменения, вносимые в рабочую программу дисциплины (модуля)

№ п/п	№ раздела внесения изменений	Дата внесения изменений	Содержание изменений	«Согласовано» заведующий кафедрой, реализующей дисциплину