Документ подписан простой электронной подписью
Информация о владельце:
ФИО: Легасова Гульназ Ильдусовна
Должность: документовед
Дата подписания: 12.07.2022 14:04:29
Уникальный программный ключ:
335064282855073467 3f401304efc033b1 0865bce4992e4e9db0cb2e7cec126c

МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ

федеральное государственное бюджетное образовательное учреждение высшего образования «Казанский национальный исследовательский технический университет им. А.Н. Туполева-КАИ»
(КНИТУ-КАИ)
Чистопольский филиал «Восток»

УТВЕРЖДАЮ
Директор ЧФ КНИТУ-КАИ
_____ И.Р.Мухаметзянов
«01» _____ 2021 г.

РАБОЧАЯ ПРОГРАММА

дисциплины

Б1.О.16 Защита информации

(индекс и наименование дисциплины по учебному плану)

Квалификация: бакалавр

(бакалавр, специалист, инженер, магистр)

Форма обучения: очная

(очная, очно-заочная, заочная)

Направление подготовки / специальность 09.03.01 Информатика и ВТ

(код и наименование направления подготовки / специальности)

Направленность (профиль)

Вычислительные машины, комплексы, системы и сети

(наименование *профиля, специализации,* магистерской программы)

Чистополь
2021 г.

Рабочая программа дисциплины разработана в соответствии с требованиями ФГОС ВО по направлению подготовки 09.03.01 Информатика и ВТ, приказом Министерства образования и науки Российской Федерации от «19» сентября 2017 г. № 929.

Разработчик:
Ефимова Ю.В., к. п.н.
(ФИО, ученая степень, ученое звание) *(подпись)*

Рабочая программа утверждена на заседании кафедры КиТС

от 25.06.2021, протокол № 8.

Заведующий кафедрой КиТС
Классен В.И., д.т.н.
(ФИО, ученая степень, ученое звание) *(подпись)*

Рабочая программа дисциплины (модуля)	Наименование подразделения	Дата	№ протокола	Подпись
ОДОБРЕНА	Кафедра КиТС	25.06.2021	8	Классен В.И.
ОДОБРЕНА	УМК филиала	29.06.2021	5	председатель УМК С.Г.Прохоров
СОГЛАСОВАНА	Научно-техническая библиотека	–	–	зав. сектором библиотеки М.А. Тугашова

1 ИСХОДНЫЕ ДАННЫЕ И КОНЕЧНЫЙ РЕЗУЛЬТАТ ИЗУЧЕНИЯ ДИСЦИПЛИНЫ

1.1 Цель изучения дисциплины

Основной целью изучения дисциплины является сформировать у студентов компетенции, связанные со знанием и пониманием сущности и значения информационной безопасности и защиты информации, определение методологических и технических основ различных аспектов защиты информации и связи между ними.

1.2 Задачи дисциплины

Основными задачами изучения дисциплины являются:

1. Формирование у обучающихся представления о теоретических основах и базовых понятиях основных типов политик безопасности и систем разграничения доступа.
2. Изучение современных методов противодействия угрозам, каналов и способов несанкционированного доступа к информации.
3. Изучение современных методов криптографической защиты информации.
4. Изучение нормативной базы в области защиты информации. Изучение типов подсистем аутентификации и идентификации.

1.3 Место дисциплины в структуре ОП ВО

Дисциплина «Защита информации» относится к обязательной части Блока 1.

1.4 Объем дисциплины 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 1.1, *а* – Объем дисциплины (модуля) для очной формы обучения

Семестр	Общая трудоемкость дисциплины (модуля), в ЗЕ/час	Виды учебной работы											
		Контактная работа обучающихся с преподавателем по видам учебных занятий (аудиторная работа), в т.ч.:							***Самостоятельная работа обучающегося (внеаудиторная работа), в т.ч.:***				
		Лекции	Лабораторные работы	Практические занятия	Курсовая работа (консультация, защита)	Курсовой проект (консультации, защита)	Консультации перед экзаменом	Контактная работа на промежуточной аттестации	Курсовая работа (подготовка)	Курсовой проект (подготовка)	Проработка учебного материала (самоподготовка)	Подготовка к промежуточной аттестации	Форма промежуточной аттестации
8	2 ЗЕ/72	32	16	-	-	-	-	0,35	-	-	23,65		зачет
Итого	**2ЗЕ/72**	**32**	**16**	**-**	**-**	**-**	**-**	**0,35**	**-**	**-**	**23,65**		

1.5 Перечень планируемых результатов обучения по дисциплине

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

Таблица 1.2 – Формируемые компетенции

Код компетенции	Наименование компетенции	Индикаторы достижения компетенций	Средства оценки
ОПК-3.	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$_{ОПК-3}$. Знает принципы, методы и средства решения стандартных задач профессиональной деятельности на основе информационной и библиографической культуры с применением информационно- коммуникационных технологий и с учетом основных требований информационной безопасности	Тестирование, устный опрос на занятии
		ИД-2$_{ОПК-3}$. Умеет решать стандартные задачи профессиональной деятельности на основе информационной и библиографической культуры с применением информационно- коммуникационных технологий и с учетом основных требований информационной безопасности	отчет по лабораторной работе, выполнение индивидуальных заданий
		ИД-3$_{ОПК-3}$. Владеет навыками подготовки обзоров, аннотаций, составления рефератов, научных докладов, публикаций и библиографии по научно- исследовательской работе с учетом требований информационной безопасности	зачет

2 СОДЕРЖАНИЕ ДИСЦИПЛИНЫ

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 и виды занятий

Наименование разделов дисциплины	Всего	Контактная работа обучающихся с преподавателем по видам учебных занятий (без промежуточной аттестации) (в час)			Самостоятельная работа (проработка учебного материала (самоподготовка))
		Лекции	Лабораторные работы	Практические занятия	
8 семестр					
1 Основные понятия	34	16	6		12
2 Методы защиты информации	38	16	10		12
Итого за семестр	**72**	**32**	**16**		**24**
Итого по дисциплине (без промежуточной аттестации)	**72**	**32**	**16**		**24**

2.2 Содержание разделов дисциплины (модуля)

1 Основные понятия

Введение. Предмет, задачи и содержание курса. Роль курса в подготовке специалиста. Связь основных разделов с другими дисциплинами учебного плана. Определение и общее содержание проблемы информационной безопасности. Три составляющие проблемы информационной безопасности. Актуальность проблемы ИБ. Методологический базис теории ИБ. Информация и информационные отношения. Субъекты информационных отношений. Свойства защищенности информации. Защита от незаконного тиражирования. Угрозы информационной безопасности и меры защиты информации. Виды угроз. Каналы несанкционированного получения информации. Модель нарушителя. Классификация мер защиты. Источники, риски и формы атак на информацию разрушающие программные средства.

2 Методы защиты информации

Политики безопасности и системы разграничения доступа. Субъектно-объектная модель КС. Идентификация, аутентификация и авторизация. Парольные системы. Монитор безопасности. Дискреционная и мандатная политики безопасности. Модель Харрисона-Руззо-Ульмана. Модель танизованной матрицы доступа. Модель Белла-Лападулы. Модели Биба и Кларка Вильсона. Методы криптографической защиты информации. Традиционные методы шифрования. Мето-

ды замены, перестановки, гаммирования. Симметричные системы. Практическая и теоретическая стойкость. Односторонние функции. Открытое распространение ключей. Ассиметричные системы. Криптосистема RSA. Электронная цифровая подпись. Стойкость ассиметричных систем. Аутентификация на основе сертификатов. Нормативное обеспечение защиты информации. Зарубежные стандарты информационной безопасности. Лицензирование, сертификация и аттестация в области защиты информации.

2.3 Курсовая работа

Не предусмотрено учебным планом.

3 ОЦЕНОЧНЫЕ МАТЕРИАЛЫ И МЕТОДИЧЕСКИЕ РЕКОМЕНДАЦИИ ПО ОСВОЕНИЮ ДИСЦИПЛИНЫ

3.1 Содержание оценочных средств и их соответствие запланированным результатам обучения

Текущий контроль успеваемости обеспечивает оценивание хода освоения дисциплины (модуля). Содержание оценочных материалов текущего контроля представлено в таблице 3.1.

Таблица 3.1 – Оценочные материалы текущего контроля

Виды учебных занятий	Наименование оценочного средства текущего контроля	Код и индикатор достижения компетенции
Лекции	Тестовые задания текущего контроля по двум разделам дисциплины, вопросы на занятиях	ИД-1$_{ОПК-3}$
Лабораторные работы	Вопросы к лабораторным работам	ИД-2$_{ОПК-3}$
Самостоятельная работа	Вопросы для самоподготовки, тестирование	ИД-1$_{ОПК-3}$, ИД-2$_{ОПК-3}$. , 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. Что из перечисленного является верным?

а) субъект доступа – это пассивный компонент, который может стать причиной потока информации от субъекта к объекту или изменения состояния системы

б) субъект доступа – это активный компонент, который может стать причиной потока информации от объекта к субъекту или изменения состояния системы

в) объект доступа – это пассивный компонент системы, не хранящий, не принимающий и не передающий информацию

г) объект доступа – это активный компонент системы, хранящий, принимающий или передающий информацию

2. Свойства информации с точки зрения информационной безопасности

а) интерпретируемость, связность, активность

б) уязвимость, угроза, атака

в) полнота и непротиворечивость

г) целостность, конфиденциальность, доступность

3. Расставьте в порядке логического следования событий в АСОИ

а) возникновение угрозы, наличие уязвимости, реализация атаки

б) наличие уязвимости, возникновение угрозы, реализация атаки

в) реализация атаки, наличие уязвимости, возникновение угрозы

г) наличие уязвимости, реализация атаки, возникновение угрозы

4. К какой мере обеспечения информационной безопасности относится использование криптографических средств преобразования информации?

а) правовая

б) программно-аппаратная

в) морально-этическая

г) организационно-административная

5. Основная цель создания политики безопасности информационной системы

а) определить множество субъектов и объектов компьютерной системы

б) наделить полномочиями пользователей информационной системы

в)определить условия, которым подчиняется поведение подсистемы безопасности

г) обеспечить целостность, конфиденциальность и доступность информации

6. Какая политика безопасности не обеспечивает конфиденциальность?

а) политика безопасности Хариссона-Руззо-Ульмана

б) политика безопасности Биба

в) политика безопасности Белла-ЛаПадулы

г) мандатная политика безопасности

7.Какая политика безопасности контролирует целостность информации?

а)политика безопасности Белла-ЛаПадулы

б)политика безопасности Хариссона-Руззо-Ульмана

в)политика безопасности Белла-ЛаПадулы

г)дискреционная политика безопасности

8. Что из перечисленного не может использоваться в системах биометрической идентификации/аутентификации пользователей?

а) рукописный почерк

б) клавиатурный почерк

в) мышиный почерк

г) крысиный почерк

9. Какая из криптоаналитических атак требует привлечения предельных вычислительных ресурсов?

а) атака методом анализа частотности закрытого текста

б) атака по словарю

в) атака по открытому тексту

г) атака методом полного перебора всех возможных ключей

10. Основной недостаток симметричной криптосистемы

а) проблема генерации ключевой информации

б) низкая скорость работы симметричных криптоалгоритмов

в) отсутствие эффективных алгоритмов симметричного шифрования

г) проблема хранения и распространения ключей шифрования

Примеры тем устных опросов на занятиях:

1. Какие виды систем средств защиты информации существуют?

2. Как функционируют ассиметричные системы шифрования?

3. Как функционирует мандатная политика безопасности ?

4. Что такое клавиатурный почерк?
5. Как работает биометрический способ аутентификации и идентификации ?
6. Какие виды каналов утечки информации существуют?

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

Примеры вопросов для самоподготовки:
1. Что такое информационная безопасность?
2. Что такое свойства информации?
3. Какими параметрами характеризуются парольные системы?
4. На чем основан принцип открытости средств защиты информации?
5. Какие существуют политики безопасности?

Полный комплект контрольных заданий или иных материалов, необходимых для оценивания результатов обучения по дисциплине (модулю), практике хранится на кафедре-разработчике в бумажном или электронном виде.

3.2 Содержание оценочных материалов промежуточной аттестации

Промежуточная аттестация обеспечивает оценивание промежуточных/ окончательных 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 тестовых заданий промежуточной аттестации:
1. Какая угроза реализуется при атаке на чтение закрытой информации?
а) нарушение конфиденциальности информации
б) нарушение доступности информации
в) нарушение целостности информации
г) нарушение работоспособности системы обработки информации
2. Что из перечисленного не является каналом утечки информации?
а) виброакустический канал
б) электромагнитный канал
в) визуальный канал
г) информационный канал
3. Понятие, не относящееся к свойствам функций хэширования
а) рассеивание
б) чувствительность к изменениям
в) открытость
г) необратимость
4. Какая политика безопасности разрешает проблему программных закладок?

а) мандатная политика безопасности
б) дискреционная политика безопасности
в) политика безопасности Хариссона-Руззо-Ульмана
г) политика безопасности Белла-ЛаПадулы

5. Какое из перечисленных определений является верным?

а) идентификация – подтверждение принадлежности аутентификатора пользователю

б) аутентификация – подтверждение принадлежности идентификатора пользователю

в) авторизация – предъявление пользователем идентификатора для идентификации

г) верификация – наделение полномочиями субъекта системы

Примеры контрольных вопросов:

1. Основные понятия и определения предмета защиты информации (понятие доступа, свойства безопасности информации, уязвимость, угроза, атака, каналы реализации угроз)
2. Принципы и меры обеспечения информационной безопасности в АСОИ
3. Понятие политики безопасности и их классификация
4. Политики избирательного разграничения доступа (модель Харрисона-Руззо-Ульмана)
5. Мандатные политики безопасности (модель Белла-ЛаПадуллы)
6. Понятие идентификации и аутентификации субъектов. Классификация подсистем идентификации и аутентификации
7. Парольные системы идентификации и аутентификации пользователей
8. Идентификация и аутентификация пользователей с использованием технических устройств
9. Идентификация и аутентификация с использованием индивидуальных биометрических характеристик пользователя
10. Функции хэширования и электронно-цифровая подпись
11. Хранение и распределение ключевой информации. Протоколы безопасной аутентификации пользователей
12. Типовые схемы хранения ключевой информации
13. Электронные ключи HASP
14. Политика безопасности контроля целостности информации (модель Биба)
15. Инфраструктура открытых ключей PKI
16. Иерархия ключевой информации
17. Подходы к распределению ключевой информации
18. Протоколы безопасной удаленной аутентификации пользователей
19. Проблема защиты программного обеспечения от несанкционированного использования
20. Модульная архитектура технических средств защиты ПО от несанкционированного использования

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 – Балльные 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		15	15	30
Итого (максимум за период)	**6**	**22**	**22**	**50**
Зачет / экзамен				**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

4.1 Учебно-методическое и информационное обеспечение дисциплины

4.1.1 Основная литература

1. Бабаш, А. В. Моделирование системы защиты информации. Практикум : учебное пособие / Е. К. Баранова, А. В. Бабаш. — 3-е изд., перераб. и доп. — Москва : РИОР : ИНФРА-М, 2020. — 320 с. — (Высшее образование). - ISBN 978-5-369-01848-4. - Текст : электронный. - URL: https://znanium.com/catalog/product/1052206 . – Режим доступа: по подписке.
2. Хорев П.Б. Методы и средства защиты информации в компьютерных системах. - 2 -е изд., стер. - М.: ИЦ "Академи", 2016. - 256 с.
3. Комплексная защита информации в корпоративных системах : учеб. пособие / В.Ф. Шаньгин. — М. : ИД «ФОРУМ» : ИНФРА-М, 2017. — 592 с. — Режим доступа: http://znanium.com/bookread2.php?book=546679

4.1.2 Дополнительная литература

1. Глинская, Е. В. Информационная безопасность конструкций ЭВМ и систем : учебное пособие / Е. В. Глинская, Н. В. Чичварин. - Москва : ИНФРА-М, 2021. - 118 с. - (Высшее образование: Специалитет). - ISBN 978-5-16-016536-3. - Текст : электронный. - URL: https://znanium.com/catalog/product/1178153 – Режим доступа: по подписке.
2. Электронный документооборот и обеспечение безопасности стандартными средствами windows : учебное пособие / Л.М. Евдокимова, В.В. Корябкин, А.Н. Пылькин, О.Г. Швечкова. – М. : КУРС, 2017. – 296 с. — Режим доступа: http://znanium.com/bookread2.php?book=851088

4.1.3 Методическая литература к выполнению практических и/или лабораторных работ

1. Методические указания для выполнения лабораторных работ по дисциплине «Защита информации» в электронном виде (библиотека ЧФ КНИТУ-КАИ).

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

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

1. Ефимова Ю.В. «Защита информации» [Электронный ресурс]: курс дистанционного обучения по направлению подготовки бакалавров 09.03.01 «Информатика и вычислительная техника» / КНИТУ-КАИ, Казань, 2017 – Доступ по логину и паролю. URL: https://bb.kai.ru:8443/webapps/blackboard/ execute/content/blankPage?cmd=view&content_id=_269601_1&course_id=_13779_1

Идентификатор курса 17_Chistopol_KiTS_YuVEfimova_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. URL: https://e.lanbook.com/.
2. Электронно-библиотечная система учебной и научной литературы. URL: http://znanium.com/.
3. Электронно-библиотечная система учебной и научной литературы. URL: https://urait.ru/.
4. Научно-техническая библиотека КНИТУ-КАИ. URL: http://library.kai.ru/.

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, занятий семинарского типа, консультаций, текущего контроля, промежуточной аттестации	Учебная мебель: столы, стулья для обучающихся; стол, стул для преподавателя, доска. Аудитория, оснащенная комплексом технических средств обучения (проектор или интерактивная доска, компьютер, система звукового сопровождения отображаемых видеоматериалов).
Лабораторные занятия	Компьютерный класс	Учебная мебель: столы, стулья для обучающихся; стол, стул для преподавателя, доска. Аудитория, оснащенная ПЭВМ объединенных в ЛВС с выходом в Интернет
Самостоятельная работа	Аудитория для самостоятельной работы	Библиотечный фонд: печатные издания и ЭБС рабочие места, оборудованные ПЭВМ с выходом в интернет (Wi-Fi), МФУ, принтер

Таблица 4.2 – Лицензионное и свободно распространяемое программное обеспечение, в том числе отечественного производства, используемое при осуществлении образовательного процесса по дисциплине

№ п/п	Наименование программного обеспечения	Производитель	Способ распространения (лицензионное или свободно распространяемое)
1	Microsoft Windows Microsoft Office Microsoft Visual Studio 2017		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;
– предоставление задания с использованием сурдоперевода.

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.

При занятиях с обучающимися **с нарушениями слуха** предусмотрено использование звукоусиливающей аппаратуры, мультимедийных средств и других технических средств приема/передачи учебной информации в доступных формах, мобильной системы преподавания для обучающихся с инвалидностью, портативной индукционной системы. Учебная аудитория, в которой занимаются обучающиеся с нарушением слуха, оборудована компьютерной техникой, аудиотехникой, видеотехникой, электронной доской, мультимедийной системой.

При занятиях с обучающимися **с нарушениями зрениями** предусмотрено использование в лекционных и учебных аудиториях возможности просмотра удаленных объектов (например, текста на доске или слайда на экране) при помощи видеоувеличителей для комфортного просмотра.

При занятиях с обучающимися **с нарушениями опорно-двигательного аппарата** используются альтернативные устройства ввода информации и другие технические средства приема/передачи учебной информации в доступных формах, мобильной системы обучения для людей с инвалидностью.

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

ЛИСТ УТВЕРЖДЕНИЯ РАБОЧЕЙ ПРОГРАММЫ ДИСЦИПЛИНЫ НА УЧЕБНЫЙ ГОД

Рабочая программа дисциплины утверждена на ведение учебного процесса в учебном году:

Учебный год	«Согласовано» зав. кафедрой ведущей	«Согласовано» зав. кафедрой выпускающей
2022/2023		
2023/2024		
2024/2025		