Рабочая программа дисциплины (модуля)*

Защищенные интернет-технологии

Направление подготовки (специальность)

10.05.03 Информационная безопасность автоматизированных систем

Направленность (профиль)

специализация N 4 "Безопасность автоматизированных систем критически важных объектов"

Присваиваемая квалификация (степень)

специалист по защите информации

Форма обучения

очная

Год набора 2025

*Рабочая программа дисциплины (модуля) адаптирована для инклюзивного обучения инвалидов и лиц с ограниченными возможностями здоровья

Челябинск 2025 г.

Содержание

1. ЦЕЛИ ОСВОЕНИЯ ДИСЦИПЛИНЫ

Цель учебной дисциплины состоит в овладении принципами обеспечения информационной безопасности автоматизированных систем, использующих в своей структуре локальные вычислительные сети, компоненты корпоративных сетей и сети интернет.

Задачи: освоение основных методов и технологий проектирования и развертывания защищённых систем в локальных вычислительных сетях, организации и управления зашифрованными соединениями, настройки межсетевого экранирования и систем обнаружения и предотвращения вторжений.

Индикаторы достижения компетенций:

ОПК-7.1. Обладает базовыми знаниями в области программирования.

ОПК-7.2. Демонстрирует умения создавать программы на языках общего назначения, применять методы и инструментальные средства программирования для решения профессиональных задач.

ОПК-7.3. Имеет практический опыт осуществлять обоснованный выбор инструментария программирования и способов организации программ.

ОПК-13.1. Обладает знаниями о диагностике, тестировании и анализе уязвимостей систем защиты информации автоматизированных систем.

ОПК-13.2. Демонстрирует умения организовывать и проводить диагностику и тестирование систем защиты информации автоматизированных систем.

ОПК-13.3. Имеет практический опыт проводить анализ уязвимостей систем защиты информации автоматизированных систем.

2. МЕСТО ДИСЦИПЛИНЫ В СТРУКТУРЕ ОПОП

Цикл (раздел) ОПОП: Б1.О.34

2.1 Требования к предварительной подготовке обучающегося:

Физика

Введение в специальность

Информатика

Организация ЭВМ и вычислительных систем

2.2 Дисциплины и практики, для которых освоение данной дисциплины (модуля) необходимо как предшествующее:

Обеспечение информационной безопасности на критически важных объектах

Безопасность сетей ЭВМ

Управление информационной безопасностью

Производственная практика (преддипломная практика)

Подготовка к сдаче и сдача государственного экзамена

Подготовка к процедуре защиты и защита выпускной квалификационной работы

3. КОМПЕТЕНЦИИ ОБУЧАЮЩЕГОСЯ, ФОРМИРУЕМЫЕ В РЕЗУЛЬТАТЕ ОСВОЕНИЯ ДИСЦИПЛИНЫ (МОДУЛЯ)

ОПК-7: Способен создавать программы на языках общего назначения, применять методы и инструментальные средства программирования для решения профессиональных задач, осуществлять обоснованный выбор инструментария программирования и способов организации программ;

Знать:

Для достижения индикатора ОПК-7.1: Знать базовые понятия в области программирования (технологию разработки web-приложений).

Уметь:

Для достижения индикатора ОПК-7.2: Уметь создавать программы на языках общего назначения, применять методы и инструментальные средства программирования для решения профессиональных задач (разрабатывать web- приложения).

Владеть:

Для достижения индикатора ОПК-7.3: Владеть навыками осуществления обоснованного выбора инструментария программирования и способов организации программ.

ОПК-13: Способен организовывать и проводить диагностику и тестирование систем защиты информации автоматизированных систем, проводить анализ уязвимостей систем защиты информации автоматизированных систем;

Знать:

Для достижения индикатора ОПК-13.1: Знать о диагностике, тестировании и анализе уязвимостей систем защиты информации автоматизированных систем (основные подходы к процессам аудита, мониторинга, самообследования и контроля СУИБ, основные приемы поиска и анализа информации, методы и технологии проектирования и развертывания защищённых систем в локальных вычислительных сетях).

Уметь:

Для достижения индикатора ОПК-13.2: Уметь организовывать и проводить диагностику и тестирование систем защиты информации автоматизированных систем (анализировать защищенность автоматизированных систем, организовывать и управлять зашифрованными соединениями, настраивать средства межсетевого экранирования, системы обнаружения и предотвращения вторжений).

Владеть:

Для достижения индикатора ОПК-13.3: Владеть навыками проведения анализа уязвимостей систем защиты информации автоматизированных систем (навыками поиска и анализа регулирующих и методических документов, навыками анализа уязвимостей систем защиты информации автоматизированных систем).

В результате освоения дисциплины обучающийся должен

3.1	**Знать:**
3.1.1	основные подходы к процессам аудита, мониторинга, самообследования и контроля СУИБ;
3.1.2	основные приемы поиска и анализа информации;
3.1.3	методы и технологии проектирования и развертывания защищённых систем в локальных вычислительных сетях
3.2	**Уметь:**
3.2.1	анализировать защищенность автоматизированных систем;
3.2.2	организовывать и управлять зашифрованными соединениями;
3.2.3	настраивать средства межсетевого экранирования, системы обнаружения и предотвращения вторжений;
3.2.4	навыками работы с научно-технической литературой по перспективным сетям и системам связи с целью повышения эффективности защищенных автоматизированных систем
3.3	**Владеть:**
3.3.1	навыками поиска и анализа регулирующих и методических документов;
3.3.2	навыками анализа уязвимостей систем защиты информации автоматизированных систем

4. ОБЪЕМ ДИСЦИПЛИНЫ (МОДУЛЯ)

Общая трудоемкость	**2 ЗЕТ**
Часов по учебному плану: 72 в том числе: аудиторные занятия: 52 самостоятельная работа: 14,7 контактная работа: 57,3 ИКР: 5,3	Виды контроля в семестрах: зачеты 5

5. СТРУКТУРА И СОДЕРЖАНИЕ ДИСЦИПЛИНЫ (МОДУЛЯ)

Код занятия	Наименование разделов и тем /вид занятия/	Семестр / Курс	Часов	Литература
	Раздел 1. Государственная система защиты информации.			
1.1	Государственная система защиты информации. /Лек/	5	2	Л1.1 Л1.2 Л1.3 Л1.4 Л1.5 Л1.6Л2.1 Э1 Э2 Э3 Э4 Э5

	Раздел 2. Локальные вычислительные сети и интернет- технологии			
2.1	Сетевые технологии. Технологии сети Интернет. /Лек/	5	2	Л1.1 Л1.2 Л1.3 Л1.4 Л1.5 Л1.6Л2.1 Э1 Э2 Э3 Э4 Э5
2.2	Проработка лекционного материала. Подготовка и оформление отчетов по лабораторным работам. Развитие технологий сети Интернет. /Ср/	5	2	Л1.1 Л1.2 Л1.3 Л1.4 Л1.5 Л1.6Л2.1 Э1 Э2 Э3 Э4 Э5
2.3	Организация локальной вычислительной сети /Лаб/	5	2	Л1.1 Л1.2 Л1.3 Л1.4 Л1.5 Л1.6Л2.1 Э1 Э2 Э3 Э4 Э5
	Раздел 3. Защищенные протоколы			
3.1	Защита данных на канальном уровне. Защита данных на сетевом и транспортном уровнях. /Лек/	5	6	Л1.1 Л1.2 Л1.3 Л1.4 Л1.5 Л1.6Л2.1 Э1 Э2 Э3 Э4 Э5
3.2	Проработка лекционного материала. Подготовка и оформление отчетов по лабораторным работам. Защищенные протоколы. История вопроса. /Ср/	5	2	Л1.1 Л1.2 Л1.3 Л1.4 Л1.5 Л1.6Л2.1 Э1 Э2 Э3 Э4 Э5
3.3	Организация и управление VPN-соединениями /Лаб/	5	2	Л1.1 Л1.2 Л1.3 Л1.4 Л1.5 Л1.6Л2.1 Э1 Э2 Э3 Э4 Э5
	Раздел 4. Основы программирования сетевых приложений			
4.1	Технология разработки web-приложений. /Лек/	5	4	Л1.1 Л1.2 Л1.3 Л1.4 Л1.5 Л1.6Л2.1 Э1 Э2 Э3 Э4 Э5
4.2	Проработка лекционного материала. Подготовка и оформление отчетов по лабораторным работам. Современные технологии разработки web-приложений. /Ср/	5	4	Л1.1 Л1.2 Л1.3 Л1.4 Л1.5 Л1.6Л2.1 Э1 Э2 Э3 Э4 Э5
4.3	Разработка web-приложений /Лаб/	5	2	Л1.1 Л1.2 Л1.3 Л1.4 Л1.5 Л1.6Л2.1 Э1 Э2 Э3 Э4 Э5
	Раздел 5. Криптографические основы сетевой безопасности			
5.1	Криптография. Симметричные алгоритмы шифрования. Асимметричные алгоритмы шифрования. /Лек/	5	6	Л1.1 Л1.2 Л1.3 Л1.4 Л1.5 Л1.6Л2.1 Э1 Э2 Э3 Э4 Э5
5.2	Анализ алгоритмов шифрования /Лаб/	5	2	Л1.1 Л1.2 Л1.3 Л1.4 Л1.5 Л1.6Л2.1 Э1 Э2 Э3 Э4 Э5
5.3	Проработка лекционного материала. Подготовка и оформление отчетов по лабораторным работам. Анализ и синтез криптоалгоритмов. /Ср/	5	4	Л1.1 Л1.2 Л1.3 Л1.4 Л1.5 Л1.6Л2.1 Э1 Э2 Э3 Э4 Э5
	Раздел 6. Аппаратно-программные средства защиты информации от несанкционированного доступа			
6.1	Защита информации от несанкционированного доступа. Защита информации от несанкционированного доступа АРМ. Аппаратно-программные системы защиты информации от НСД. /Лек/	5	10	Л1.1 Л1.2 Л1.3 Л1.4 Л1.5 Л1.6Л2.1 Э1 Э2 Э3 Э4 Э5
6.2	Аппаратно-программные системы защиты информации от НСД /Лаб/	5	2	Л1.1 Л1.2 Л1.3 Л1.4 Л1.5 Л1.6Л2.1 Э1 Э2 Э3 Э4 Э5
6.3	Проработка лекционного материала. Подготовка и оформление отчетов по лабораторным работам. /Ср/	5	2	Л1.1 Л1.2 Л1.3 Л1.4 Л1.5 Л1.6Л2.1 Э1 Э2 Э3 Э4 Э5

	Раздел 7. Аппаратно-программные средства защиты информации и управления сетью			
7.1	Аппаратно-программные средства защиты информации и управления сетью. /Лек/	5	4	Л1.1 Л1.2 Л1.3 Л1.4 Л1.5 Л1.6Л2.1 Э1 Э2 Э3 Э4 Э5
7.2	Обзор технологий и развертывание системы защиты. Сервер доступа и центр управления сетью. Правила фильтрации IP-пакетов и правила трансляции. Мониторинг и диагностика системы защиты. /Лаб/	5	8	Л1.1 Л1.2 Л1.3 Л1.4 Л1.5 Л1.6Л2.1 Э1 Э2 Э3 Э4 Э5
7.3	Проработка лекционного материала. Подготовка и оформление отчетов по лабораторным работам. /Ср/	5	0,7	Л1.1 Л1.2 Л1.3 Л1.4 Л1.5 Л1.6Л2.1 Э1 Э2 Э3 Э4 Э5
	Раздел 8. Иная контактная работа			
8.1	Индивидуальные консультации, текущий контроль /ИКР/	5	5,3	Л1.1 Л1.2 Л1.3 Л1.4 Л1.5 Л1.6Л2.1 Э1 Э2 Э3 Э4 Э5

6. ФОНД ОЦЕНОЧНЫХ СРЕДСТВ

6.1. Перечень видов оценочных средств

Собеседование и отчеты по лабораторным работам.
Зачет

6.2. Типовые контрольные задания и иные материалы для текущей аттестации

Вопросы для собеседования по лабораторным работам:
1) Нормативно-правовые акты в сфере информационной безопасности, действующие на территории Российской Федерации;
2) Государственные стандарты в области защиты информации и сетевых технологий;
3) Криптографические стандарты и средства, базовые технологии обеспечения информационной безопасности;
4) Анализ защищенности автоматизированных систем;
5) Базовые технологии проектирования систем мониторинга средств защиты информации;
6) Разработке защищенных автоматизированных систем в сфере профессиональной деятельности;
6) Оценка эффективности средств защиты информации, использующихся на критически важных объектах и в автоматизированных системах критически важных объектов;
7) Проектировании средств защиты информации автоматизированной системы;
8) Эффективное применение средств защиты информационно-технологических ресурсов автоматизированной системы и восстановление их работоспособности при возникновении нештатных ситуаций;
9) Проектирование, внедрение и использование системы мониторинга средств защиты информации, функционирующих на критически важных объектах и в автоматизированных системах критически важных объектов.

6.3. Типовые контрольные вопросы и задания для промежуточной аттестации

Вопросы к зачету:
1. Государственная система защиты информации. Правовое и методическое обеспечение в области защиты информации.
2. Эталонная модель TCP/IP. Эталонная модель RM OSI. Стандартизация технологий сети Интернет (RFC).
3. Схема адресации в сети Интернет. Числовые адреса IPv4, IPv6. TCP адреса и UDP-адреса. Адресация сервисов. Символические адреса, DNS-серверы.
4. Базовые протоколы Протоколы IP, ICMP, UDP.
5. Протоколы маршрутизации. Основные характеристики протоколов RIP, OSPF, IGRP, EGP, BGP.
6. Socket API - прикладной программный интерфейс для программирования сетевых приложений. Понятие гнезда (socket). Примеры функций Socket API.
7. Криптографические основы сетевой безопасности. Криптография. Криптоанализ. Сеть Фейштеля. Критерии разработки криптоалгоритмов.
8. Криптографические алгоритмы защиты информации. Понятия симметричного шифрования, открытого ключа, хэш - функции, электронной подписи, примеры. Понятие инфраструктуры открытых ключей и проблемы ее создания.
9. Назначение и особенности применения алгоритмов DES и 3DES, Blowfish, IDEA, ГОСТ 28147, ГОСТ Р 34.12. Алгоритмы симметричного шифрования.
10. Создание случайных чисел. Алгоритм AES. Алгоритм Rijndael. Алгоритм RC6.
11. Алгоритмы асиммитричного шифрования. Diffie-Hellman, RSA.
12. Хэш-функции. Алгоритмы SHA и MD5.

13. Цифровая подпись. Прямая и арбитражная цифровые подписи. Стандарт цифровой подписи DSS. Отечественный стандарт цифровой подписи ГОСТ 34.10.
14. Алгоритм цифровой подписи на основе эллиптических кривых ECDSA.
15. Шифрование/дешифрование с использованием эллиптических кривых.
16. Протоколы защищенной передачи данных. Назначение протоколов SSL, SSH, PGP, IPSec, PPTP, L2TP.
17. Автоматизированное рабочее место в информационной системе. Защита конечных точек. Аппаратно- программные системы защиты информации от НСД, обеспечения доверенной загрузки.
18. Аппаратно-программные средства защиты информации и управления сетью. Сервер доступа и центр управления сетью. Криптошлюз. Криптографический коммутатор. Детектор атак.
19. Межсетевые экраны. Классификация, классы защищенности. Реализация МСЭ на канальном и сетевом уровнях. Шлюзы сеансового уровня. Посредники прикладного уровня. Типы окружений для МСЭ. DMZ-сети, конфигурации с одной и двумя DMZ-сетями.

6.4. Критерии оценивания

Критерии оценивания собеседования и отчета по лабораторным работам:
В процессе выполнения лабораторной работы каждый студент составляет индивидуальный отчет, который включает расчетную часть, а также аналитическую часть и выводы. По подготовленному отчету проводится собеседование.
Лабораторная работа засчитывается студенту, если он представил правильно оформленный отчет; владеет методикой обработки данных; усвоил теоретический материал по данной теме (последовательно, грамотно и логически стройно его излагает, уверенно отвечает на вопросы). Допускаются несущественные неточности в оформлении и ответах на вопросы.
Лабораторная работа не засчитывается студенту в случаях: наличия ошибок в расчетах, неправильного оформления отчета, искажающего смысл задания, существенных ошибок при ответах на вопросы.

Критерии оценивания зачета:
Студент допускается к зачету по дисциплине в случае выполнения им учебного плана по дисциплине (выполненных и защищенных работ). В случае наличия учебной задолженности студент отрабатывает пропущенные занятия в форме, предложенной преподавателем и представленной в настоящей программе.
Зачет проводится по билетам в устной форме. Студент выбирает билет в случайном порядке. Время подготовки студента для устного ответа на зачете должно составлять не менее 40 минут, время ответа – не более 20 минут. При подготовке и ответе на вопросы билета студент должен вести необходимые записи в листе устного ответа, который по окончании зачета подписывается студентом, сдаётся преподавателю и сохраняется им до окончания экзаменационной сессии. Проявленные студентом в ходе зачета знания оцениваются словами «зачтено», «не зачтено».
«Зачтено» выставляется:
1) содержание материала билета раскрыто полностью;
2) материал изложен грамотно, в определенной логической последовательности, точно используется терминология;
3) показано умение иллюстрировать теоретические положения конкретными примерами, применять их в новой ситуации;
4) продемонстрировано усвоение ранее изученных сопутствующих вопросов;
5) ответ самостоятельный, без наводящих вопросов;
6) допущены одна–две неточности при освещении второстепенных вопросов, которые исправляются после замечаний или наводящих вопросов.
«Не зачтено» выставляется:
1) не раскрыто основное содержание учебного материала;
2) обнаружено незнание или непонимание большей или наиболее важной части учебного материала;
3) допущены ошибки в определении понятий, при использовании терминологии, которые не исправлены после нескольких наводящих вопросов.

7. УЧЕБНО-МЕТОДИЧЕСКОЕ И ИНФОРМАЦИОННОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ (МОДУЛЯ)

7.1. Рекомендуемая литература

7.1.1. Основная литература

	Авторы, составители	Заглавие	Издательство, год	Ресурс
Л1.1	Куняев Н. Н.	Правовое обеспечение национальных интересов Российской Федерации в информационной сфере: монография (https://biblioclub.ru/index.php?page=book&id=84990)	Москва : Логос, 2010	ЭБС
Л1.2	Мельников В.П., Куприянов А.И., Мельников В.П.	Информационная безопасность: учебник (https://book.ru/book/955528)	Москва : КноРус, 2025	ЭБС
Л1.3	Лапонина О. Р.	Межсетевое экранирование: учебное пособие (https://biblioclub.ru/index.php?page=book&id=233109)	Москва : Интернет-Университет Информационных Технологий (ИНТУИТ) |Бином. Лаборатория знаний, 2007	ЭБС
Л1.4	Лапонина О. Р.	Криптографические основы безопасности: учебное пособие (https://biblioclub.ru/index.php?page=book&id=429092)	Москва : Национальный Открытый Университет «ИНТУИТ», 2016	ЭБС
Л1.5	Лапонина О. Р.	Межсетевые экраны: учебное пособие (https://biblioclub.ru/index.php?page=book&id=429093)	Москва : Национальный Открытый Университет «ИНТУИТ», 2016	ЭБС
Л1.6	Хорев П. Б.	Программно-аппаратная защита информации: учебное пособие (https://znanium.com/catalog/document?id=397282)	Москва : ООО "Научно-издательский центр ИНФРА-М", 2022	ЭБС

7.1.2. Дополнительная литература

	Авторы, составители	Заглавие	Издательство, год	Ресурс
Л2.1	Жигулин Г. П.	Организационное и правовое обеспечение информационной безопасности (https://e.lanbook.com/books/element.php?pl1_id=70952)	Санкт- Петербург : НИУ ИТМО, 2014	ЭБС

7.2. Перечень ресурсов информационно-телекоммуникационной сети "Интернет"

Э1	Лань [Электронный ресурс] : электронно-библиотечная система (ЭБС) / издательство Лань. – URL: http://e.lanbook.com/
Э2	Университетская библиотека онлайн [Электронный ресурс] : электронно-библиотечная система (ЭБС) / ООО Директмедиа Паблишинг. – URL: http://biblioclub.ru/
Э3	Юрайт [Электронный ресурс] : электронно-библиотечная система (ЭБС) / издательство Юрайт. - URL: https://urait.ru/
Э4	Znanium.com [Электронный ресурс] : электронно-библиотечная система (ЭБС) / Научно-издательский центр ИНФРА-М. – URL: http://znanium.com/
Э5	eLIBRARY.RU [Электронный ресурс] : электронная библиотека / Науч. электрон. б-ка. – URL: http://elibrary.ru/defaultx.asp

7.3 Перечень информационных технологий

7.3.1 Программное обеспечение

OpenOffice

Notepad++

VirtualBox

Visual Studio

LMS Moodle

Adobe Connect Acrobat

ПО Kaspersky

7.3.2 Профессиональные базы данных и информационно-справочные системы

1. Электронный каталог научной библиотеки ЧелГУ [Электронный ресурс] : база данных / Челяб. гос. ун-т. – Челябинск, 1992.

2. APS JOURNALS. Physical Review Letters, Physical Review X, Physical Review, and Reviews of Modern Physics : журналы American Physical Society : сайт. – URL: http://journals.aps.org/about – Яз. англ. – Режим доступа: только из сети университета. – Текст : электронный.

3. Web of Science : мультидисциплинарная реферативная база данных / компания Thomson Reuters. – Режим доступа: для зарегистрир. пользователей ЧелГУ. – Текст : электронный.

4. Scopus : реферативная база данных / Elsevier BV. – URL: http://www.scopus.com/ – Яз. англ. – Режим доступа: для зарегистрир. пользователей ЧелГУ. – Текст : электронный.

5. Springer Link : [сайт]. – URL: http://link.springer.com/ – Яз. англ. – Режим доступа: для зарегистрир. пользователей ЧелГУ. – Текст : электронный.

8. МАТЕРИАЛЬНО-ТЕХНИЧЕСКОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ (МОДУЛЯ)

Для реализации дисциплины используются учебные аудитории для проведения занятий лекционного типа, для проведения занятий семинарского типа, для проведения групповых и индивидуальных консультаций, для текущего контроля и промежуточной аттестации, для выполнения курсовых работ, а также аудитории для самостоятельной работы.

Учебные аудитории укомплектованы специализированной мебелью и техническими средствами обучения - мультимедийным оборудованием (экран, ноутбук, проектор, колонки).

Для проведения занятий лекционного типа предлагаются наборы демонстрационного оборудования и учебно- наглядных пособий (мультимедийные презентации), различные формы наглядности (графики, таблицы, схемы и т.д)).

Лабораторные занятия проходят в учебной лаборатории электроники и схемотехники, микропроцессорных систем (аудитория 221 учебный корпус №1). Материально - техническое обеспечение приведено в паспорте лаборатории.

Для самостоятельной работы студента используются аудитория №205 - читальный зал №3 (учебный корпус №1) и аудитория №206 - электронный читальный зал (специализированный медиацентр) (учебный корпус №1), оснащенные персональными компьютерами, мультимедийной аппаратурой. В аудиториях обеспечен доступ к различной справочной литературе, энциклопедиям, библиографическим и полнотекстовым базам данных, информационным ресурсам «Интернет».

9. МЕТОДИЧЕСКИЕ УКАЗАНИЯ ДЛЯ ОБУЧАЮЩИХСЯ ПО ОСВОЕНИЮ ДИСЦИПЛИНЫ (МОДУЛЯ)

Освоение содержания учебной дисциплины «Защищенные интернет-технологии» осуществляется на лекциях, лабораторных занятиях и в процессе самостоятельной учебной деятельности студентов.

Лекции составляют основу теоретической подготовки студентов с целью понимания ими сущности дисциплины. Лекционные занятия посвящены рассмотрению ключевых, базовых положений дисциплины и разъяснению учебных заданий, выносимых на самостоятельную проработку. В ходе лекционных занятий нужно конспектировать учебный материал, обращать внимание на категории, формулировки, раскрывающие содержание тех или иных явлений и процессов, задавать преподавателю уточняющие вопросы с целью уяснения теоретических положений. Лекции должны активизировать познавательную деятельность обучающихся, вызывать интерес к поставленным проблемам и направлениям развития в профессиональной области, формировать их профессиональный кругозор, аналитические качества, творческий подход к изучению дисциплины, определять направления дальнейшего самостоятельного изучения и практического освоения в данной области. Изложение материала лекций должно носить проблемный, инновационный характер, способствующий формированию и развитию соответствующих компетенций. Преподавателю необходимо опираться на основную литературу, представленную в рабочей программе данной дисциплины, а также на учебные пособия, монографии, научные статьи и периодические издания известных специалистов в данной области.

Лабораторные работы предназначены для приобретения опыта практической реализации полученных теоретических знаний. Указания к лабораторным работам прорабатываются студентами во время самостоятельной подготовки. Необходимый уровень подготовки контролируется преподавателем перед проведением лабораторных работ. На лабораторных занятиях студенты овладевают первоначальными профессиональными умениями и навыками, которые в дальнейшем закрепляются и совершенствуются в процессе прохождения учебной и производственной практик.

Самостоятельная работа студентов включает проработку лекционного курса, подготовку к лабораторным работам, выполнение всех заявленных в рабочей программе видов самостоятельной работы (выполнение домашних заданий). Самостоятельная работа предусматривает не только проработку материалов лекционного курса, но и их расширение в результате поиска, анализа, структурирования и представления в компактном виде современной информации из всех возможных источников. В ходе самостоятельной работы необходимо изучить основную литературу, ознакомиться с дополнительной литературой. Очень полезно дорабатывать свой конспект лекций, делая в нем соответствующие записи из литературы, рекомендованной преподавателем и предусмотренной рабочей программой.

В случае применения при обучении дисциплины электронного обучения, дистанционных образовательных технологий общение обучающихся и преподавателя осуществляется в режиме реального времени (онлайн-лекции (вебинары), чаты, видео-конференции и др.) или отложенного времени (система дистанционного обучения Moodle, MS Office365, форумы, электронная почта и др.).

При обучении инвалидов и лиц с ограниченными возможностями здоровья электронное обучение, дистанционные образовательные технологии предусматривают возможность приема-передачи информации в доступных для них формах.

Реализация дисциплины с применением электронного обучения, дистанционных образовательных технологий (далее – ЭО, ДОТ) осуществляется на основании «Положения о реализации основных и дополнительных образовательных программ с применением электронного обучения и дистанционных образовательных технологий в федеральном государственном бюджетном образовательном учреждении высшего образования «Челябинский государственный университет», «Положения о порядке зачета обучающимися по основным профессиональным образовательным программам высшего образования в ФГБОУ ВО «ЧелГУ» результатов освоения в организациях, осуществляющих образовательную деятельность, учебных предметов, курсов, дисциплин (модулей), практик, дополнительных образовательных программ» посредством электронной информационно-образовательной среды ФГБОУ ВО «ЧелГУ». В исключительных случаях (форс-мажор и т.п.) при реализации образовательной деятельности с применением ЭО, ДОТ могут применять компоненты, не входящие в перечень электронной информационно-образовательной среды.

10. СПЕЦИАЛЬНЫЕ УСЛОВИЯ ОСВОЕНИЯ ДИСЦИПЛИНЫ ОБУЧАЮЩИМИСЯ С ИНВАЛИДНОСТЬЮ И ОГРАНИЧЕННЫМИ ВОЗМОЖНОСТЯМИ ЗДОРОВЬЯ

Освоение дисциплины инвалидами и лицами с ограниченными возможностями здоровья осуществляется с использованием специальных технических средств и информационных технологий, предоставляемых Ресурсным учебно-методическим центром по обучению инвалидов и лиц с ограниченными возможностями здоровья ЧелГУ по запросу обучающегося (мобильные специальные технические средства для лиц с нарушениями зрения и с нарушением слуха, ассистивные информационные технологии).

При необходимости для обучающихся с нарушениями зрения на рабочих местах для проведения практических или лабораторных занятий устанавливается специальное программное обеспечение (программа речевой навигации, речевые синтезаторы, экранные лупы).

В учебные аудитории обеспечивается беспрепятственный доступ для обучающихся с инвалидностью и с ограниченными возможностями здоровья. В каждой аудитории, где обучаются инвалиды и лица с ограниченными возможностями здоровья, предусматривается соответствующее количество мест для обучающихся с учетом нарушений их здоровья.

Для освоения дисциплины инвалидам и лицам с ограниченными возможностями здоровья предоставляется доступ к печатным источникам, имеющимся в научной библиотеке ЧелГУ, с помощью специальных технических средств; доступ с помощью специальных технических и программных средств к электронным источникам, представленным в форме электронного документа в фонде научной библиотеки ЧелГУ или электронно-библиотечных системах.

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

Для инвалидов и лиц с ограниченными возможностями здоровья освоение дисциплины может быть частично или полностью осуществлено с использованием дистанционных образовательных технологий.

При проведении промежуточной аттестации по дисциплине обучающимся с инвалидностью и с ограниченными возможностями здоровья обеспечивается по их заявлению предоставление в доступной форме в зависимости от их индивидуальных особенностей инструкции о порядке проведения промежуточной аттестации, оценочных средств и возможности ответов на задания (письменно на бумаге, набор ответов на компьютере, письменно шрифтом Брайля, с использованием услуг ассистента, устно).

При проведении процедуры оценивания результатов обучения инвалидов и лиц с ограниченными возможностями здоровья предусматривается использование предоставленных ЧелГУ или собственных технических средств, необходимых им в связи с их индивидуальными особенностями. При необходимости инвалидам и лицам с ограниченными возможностями здоровья предоставляется дополнительное время для подготовки ответа на задания, процедура оценивания результатов обучения по дисциплине может проводиться в несколько этапов.

Рабочая программа дисциплины (модуля) одобрена и рекомендована:
Проректор по учебной работе утверждено 24.02.25 А.А. Саламатов

Ученым советом физического факультета

Протокол заседания № 05 от 06.02.2025

Председатель Ученого совета
физического факультета согласовано М.А. Загребин

Заседанием кафедры радиофизики и электроники

Протокол заседания № 07 от 04.02.2025

Заведующий кафедрой согласовано А.В. Бутаков

Автор (составитель) А.В. Бутаков

Структура рабочей программы соответствует приказу ректора ФГБОУ ВО «ЧелГУ» от «13» апреля 2021 г. № 247-1