

Документ подписан простой электронной подписью	МИНОВЕР НАУКИ РОССИИ	
Информация о владельце:	Федеральное государственное бюджетное образовательное	
ФИО: Таскаев Сергей Валерьевич	учреждение высшего образования	
Должность: Ректор	«Челябинский государственный университет» (ФГБОУ ВО «ЧелГУ»)	
Дата подписания: 04.06.2025 12:35:17	Рабочая программа дисциплины "Основы построения защищенных компьютерных сетей" по направлению	стр. 1
Уникальный программный ключ:	подготовки (специальности) 10.05.01 "Компьютерная безопасность" направленности (профилю) специализация	
04c19ed8b698f7b6cb77a486b9a8788b87237373	№ 6 "Информационно-аналитическая и техническая экспертиза компьютерных систем" ФГБОУ ВО «ЧелГУ»	

## **Рабочая программа дисциплины (модуля)\*** **Основы построения защищенных компьютерных сетей**

Направление подготовки (специальность)

10.05.01 Компьютерная безопасность

Направленность (профиль)

специализация № 6 "Информационно-аналитическая и техническая экспертиза компьютерных систем"

Присваиваемая квалификация (степень)

специалист по защите информации

Форма обучения

очная

Год(ы) набора

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

Челябинск 2025 г.



## Содержание

1. Цели освоения дисциплины
2. Место дисциплины в структуре ОПОП
3. Компетенции обучающегося, формируемые в результате освоения дисциплины (модуля)
4. Объем дисциплины (модуля)
5. Структура и содержание дисциплины (модуля)
6. Фонд оценочных средств
  - 6.1. Перечень видов оценочных средств
  - 6.2. Типовые контрольные задания и иные материалы для текущей аттестации
  - 6.3. Типовые контрольные вопросы и задания для промежуточной аттестации
  - 6.4. Критерии оценивания
7. Учебно-методическое и информационное обеспечение дисциплины (модуля)
  - 7.1. Рекомендуемая литература
  - 7.2. Перечень ресурсов информационно-телекоммуникационной сети "Интернет"
  - 7.3. Перечень информационных технологий
8. Материально-техническое обеспечение дисциплины (модуля)
9. Методические указания для обучающихся по освоению дисциплины (модуля)
10. Специальные условия освоения дисциплины обучающимися с инвалидностью и ограниченными возможностями здоровья



### 1. ЦЕЛИ ОСВОЕНИЯ ДИСЦИПЛИНЫ

Цель преподавания дисциплины – обучить студентов принципам построения систем защиты информации в вычислительной сети предприятия и в процессе передачи её по сетям.

Результаты обучения по дисциплине направлены на достижение индикаторов:

ОПК-9.1 Знает методы защиты и средства обеспечения безопасности в операционных системах, компьютерных сетях и системах управления базами данных; методы предотвращения и обнаружения вторжений в операционных системах, компьютерных сетях и системах управления базами данных.

ОПК-9.2 Умеет осуществлять меры противодействия нарушениям безопасности в операционных системах, компьютерных сетях и системах управления базами данных с использованием различных программных и аппаратных средств защиты.

ОПК-16.1 Знает средства и методы хранения и передачи аутентификационной информации; механизмы реализации атак в сетях ТСР/ІР; основные протоколы идентификации и аутентификации абонентов сети; защитные механизмы и средства обеспечения сетевой безопасности; средства и методы предотвращения и обнаружения вторжений.

ОПК-16.2 Умеет формулировать и настраивать политику безопасности основных операционных систем, а также локальных компьютерных сетей, построенных на их основе; применять защищенные протоколы, межсетевые экраны и средства обнаружения вторжений для защиты информации в сетях; осуществлять меры противодействия нарушениям сетевой безопасности с использованием различных программных и аппаратных средств защиты.

ОПК-16.3 Владеет навыками настройки межсетевых экранов.

### 2. МЕСТО ДИСЦИПЛИНЫ В СТРУКТУРЕ ОПОП

Цикл (раздел) ОПОП: Б1.О.26

#### 2.1 Требования к предварительной подготовке обучающегося:

Компьютерные сети

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

Знания и практические навыки, полученные в курсе «Основы построения защищенных компьютерных сетей», расширяют профессиональный кругозор, используются обучающимися при разработке выпускных квалификационных работ, а также для подготовки и сдачи государственного экзамена.

Технологическая 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-9: Способен решать задачи профессиональной деятельности с учетом текущего состояния и тенденций развития методов защиты информации в операционных системах, компьютерных сетях и системах управления базами данных, а также методов и средств защиты информации от утечки по техническим каналам, сетей и систем передачи информации;**

#### Знать:

- иметь представление о построения современной системы защиты вычислительной сети предприятия;
- знать основы средств и методов реализации атак на сетевые ресурсы;
- знать основы принципов использования межсетевых экранов (МЭ);
- знать основы построения систем адаптивной безопасности в вычислительных сетях;
- знать основы построения виртуальных частных сетей;
- стандарты по оценке защищенных сетевых систем и их теоретические основы; методы и средства проектирования, реализации и оценки защищенных сетевых систем.

#### Уметь:

- строить системы адаптивной безопасности в вычислительных сетях;
- применять стандарты по оценке защищенных сетевых систем при анализе и проектировании систем защиты



Рабочая программа дисциплины "Основы построения защищенных компьютерных сетей" по направлению подготовки (специальности) 10.05.01 "Компьютерная безопасность" направленности (профилю) специализация N 6 "Информационно-аналитическая и техническая экспертиза компьютерных систем" ФГБОУ ВО «ЧелГУ»

стр. 4

информации.

**Владеть:**

- навыком работы построения систем адаптивной безопасности в вычислительных сетях;
- навыком работы построением виртуальных частных сетей;
- методами анализа сетевых автоматизированных систем с точки зрения обеспечения информационной безопасности.

**ОПК-16: Способен проводить мониторинг работоспособности и анализ эффективности средств защиты информации в компьютерных системах и сетях;**

**Знать:**

- угрозы и методы нарушения информационной безопасности сетевых автоматизированных систем;
- типовые модели атак, направленных на преодоление защиты сетевых автоматизированных систем;
- условия их осуществимости, возможные последствия, способы предотвращения.

**Уметь:**

- устанавливать и обслуживать современные программно-аппаратные средства обеспечения информационной безопасности компьютерных систем.

**Владеть:**

- навыками применения основных программных и аппаратных средств, необходимых для реализации систем защиты информации в сетях.

**В результате освоения дисциплины обучающийся должен**

<b>3.1 Знать:</b>	
3.1.1	– иметь представление о построения современной системы защиты вычислительной сети предприятия;
3.1.2	– знать основы средств и методов реализации атак на сетевые ресурсы;
3.1.3	– знать основы принципов использования межсетевых экранов (МЭ);
3.1.4	– знать основы построения систем адаптивной безопасности в вычислительных сетях;
3.1.5	– знать основы построения виртуальных частных сетей.
<b>3.2 Уметь:</b>	
3.2.1	– строить системы адаптивной безопасности в вычислительных сетях.
<b>3.3 Владеть:</b>	
3.3.1	– построения систем адаптивной безопасности в вычислительных сетях;
3.3.2	– построения виртуальных частных сетей.

**4. ОБЪЕМ ДИСЦИПЛИНЫ (МОДУЛЯ)**

<b>Общая трудоемкость</b>	<b>4 ЗЕТ</b>
Часов по учебному плану : 144 в том числе : аудиторные занятия : 68 самостоятельная работа : 69,1 : контактная работа: 74,9 ИКР: 6,9	Виды контроля в семестрах:  зачеты 7

**5. СТРУКТУРА И СОДЕРЖАНИЕ ДИСЦИПЛИНЫ (МОДУЛЯ)**

Код занятия	Наименование разделов и тем /вид занятия/	Семестр / Курс	Часов	Литература
	<b>Раздел 1. Сетевые модели OSI и TCP/IP</b>			
1.1	Сетевые модели OSI и TCP/IP. Стек протоколов OSI. Стек протоколов TCP/IP. Межуровневые взаимодействия. Горизонтальная и вертикальная модель OSI. Терминология инкапсуляции. Физический уровень. Канальный уровень. Сетевой уровень. Транспортный уровень. Адресация в протоколе IP. /Лек/	7	6	Л1.1 Л1.2 Л1.3Л2.1 Л2.2 Л2.3



Рабочая программа дисциплины "Основы построения защищенных компьютерных сетей" по направлению подготовки (специальности) 10.05.01 "Компьютерная безопасность" направленности (профилю) специализация N 6 "Информационно-аналитическая и техническая экспертиза компьютерных систем" ФГБОУ ВО «ЧелГУ»				стр. 5
1.2	Изучение сетевых анализаторов трафика. /Лаб/	7	6	Л1.1 Л1.2 Л1.3Л2.1 Л2.2 Л2.3
1.3	Сетевые модели OSI и TCP/IP /Ср/	7	10	Л1.1 Л1.2 Л1.3Л2.1 Л2.2 Л2.3
<b>Раздел 2. Атаки на сетевые службы</b>				
2.1	Атаки на сетевые службы. Основные понятия компьютерной безопасности. Классификация удаленных атак на распределенные вычислительные системы. Характеристика и механизмы реализации типовых удаленных атак Примеры удаленных атак на хосты. /Лек/	7	6	Л1.1 Л1.2 Л1.3Л2.1 Л2.2 Л2.3
2.2	Атаки на сетевые службы. /Лаб/	7	6	Л1.1 Л1.2 Л1.3Л2.1 Л2.2 Л2.3
2.3	Атаки на сетевые службы /Ср/	7	14	Л1.1 Л1.2 Л1.3Л2.1 Л2.2 Л2.3
<b>Раздел 3. Адаптивная безопасность в ВС</b>				
3.1	Адаптивная безопасность в ВС. Концепция адаптивного управления безопасностью. Технологии обнаружения вторжений. Технологии обнаружения вторжений /Лек/	7	6	Л1.1 Л1.2 Л1.3Л2.1 Л2.2 Л2.3
3.2	Изучение сканеров сетевой безопасности. /Лаб/	7	6	Л1.1 Л1.2 Л1.3Л2.1 Л2.2 Л2.3
3.3	Адаптивная безопасность в ВС /Ср/	7	15,1	Л1.1 Л1.2 Л1.3Л2.1 Л2.2 Л2.3
<b>Раздел 4. Технологии межсетевых экранов</b>				
4.1	Технологии межсетевых экранов. Межсетевые экраны. Функции межсетевых экранов. Функционирование МЭ на различных уровнях OSI. Варианты исполнения межсетевых экранов. Схемы сетевой защиты на базе межсетевых экранов. /Лек/	7	8	Л1.1 Л1.2 Л1.3Л2.1 Л2.2 Л2.3
4.2	Изучение межсетевых экранов. /Лаб/	7	8	Л1.1 Л1.2 Л1.3Л2.1 Л2.2 Л2.3
4.3	Технологии межсетевых экранов /Ср/	7	15	Л1.1 Л1.2 Л1.3Л2.1 Л2.2 Л2.3
<b>Раздел 5. Основы технологий виртуальных сетей.</b>				
5.1	Основы технологий виртуальных сетей. Основы технологий виртуальных защищенных сетей. Концепция построения виртуальных частных сетей. Средства обеспечения безопасности VPN. Классификация сетей VPN. Протоколы формирования защищенных каналов на канальном уровне. Протоколы формирования защищенных каналов на сеансовом уровне. Протокол формирования защищенных каналов на сетевом уровне. Протоколы АН и ESP. /Лек/	7	8	Л1.1 Л1.2 Л1.3Л2.1 Л2.2 Л2.3
5.2	Проектирование и построение VPN. /Лаб/	7	8	Л1.1 Л1.2 Л1.3Л2.1 Л2.2 Л2.3
5.3	Основы технологий виртуальных защищенных сетей /Ср/	7	15	Л1.1 Л1.2 Л1.3Л2.1 Л2.2 Л2.3
<b>Раздел 6. Иная контактная работа</b>				



Рабочая программа дисциплины "Основы построения защищенных компьютерных сетей" по направлению подготовки (специальности) 10.05.01 "Компьютерная безопасность" направленности (профилю) специализация N 6 "Информационно-аналитическая и техническая экспертиза компьютерных систем" ФГБОУ ВО «ЧелГУ»

стр. 6

6.1	Иная контактная работа: индивидуальные консультации, текущий контроль. /ИКР/	7	6,9	Л1.1 Л1.2 Л1.3Л2.2 Л2.1 Л2.3
-----	--	---	-----	---------------------------------

## 6. ФОНД ОЦЕНОЧНЫХ СРЕДСТВ

### 6.1. Перечень видов оценочных средств

Лабораторная работа.

Перечень вопросов к зачету.

### 6.2. Типовые контрольные задания и иные материалы для текущей аттестации

Лабораторный практикум (лабораторные работы №1-3)

№ п/п Наименование лабораторных работ

- 1 Изучение сетевых анализаторов трафика.
- 2 Атаки на сетевые службы.
- 3 Изучение сканеров сетевой безопасности.

### 6.3. Типовые контрольные вопросы и задания для промежуточной аттестации

Список вопросов к зачёту

1. Стек протоколов OSI, TCP/IP.
2. Основные понятия компьютерной безопасности.
3. Характеристика и механизмы реализации типовых удаленных атак.
4. Примеры сетевых атак.
5. Анализ защищенности и обнаружение атак.
6. Основные элементы адаптивной безопасности.
7. Технология обнаружения атак.
8. Межсетевой экран.
9. Функции межсетевых экранов.
10. Основные понятия и функции сети VPN.
11. Варианты построения виртуальных защищенных каналов.
12. Классификация сетей VPN.
13. Протоколы формирования защищенных каналов на канальном уровне.
14. Протоколы формирования защищенных каналов на сеансовом уровне.
15. Протокол формирования защищенных каналов на сетевом уровне.
16. Протоколы АН и ESP.

### 6.4. Критерии оценивания

В течение семестра проводятся три лабораторные работы. Максимальный балл за выполнение одной лабораторной работы – 5 баллов.

На зачете студент в письменной форме дает развернутый ответ на 2 теоретических вопроса из списка, вытянутых в случайном порядке в виде билета. Затем в устной форме отвечает на дополнительные вопросы преподавателя и дает все необходимые пояснения. Время на подготовку ответа – 40 минут, время на устный ответ – 5 минут. К полученным за ответ баллам прибавляются баллы за выполненные в ходе учебного процесса лабораторные работы.

Максимальный балл за ответ на один теоретический вопрос из билета — 15 баллов.

Максимальный балл за билет – 30 баллов.

Сводная таблица рейтинга успеваемости

№ Перечень контрольных мероприятий в семестре Максимальное кол-во баллов

1	Лабораторная работа №1-3	3x5=15
2	Зачет	2x15=30
3	Итого	45

Критерии оценивания лабораторных работ

Максимальный балл за выполнение одной лабораторной работы – 5 баллов.

Отлично/Зачтено/5 баллов - Работа выполнена в срок, обучающийся отлично знает материал, умеет анализировать проблему и может грамотно прокомментировать выполненную работу.

Хорошо/зачтено/3-4 балла - Работа выполнена в срок, обучающийся хорошо знает материал, умеет анализировать проблему и может грамотно прокомментировать выполненную работу. Обучающийся допускает незначительные ошибки.

Удовлетворительно/зачтено/1-2 балла - Работа выполнена и сдана позднее, чем предполагалось. Обучающийся



Рабочая программа дисциплины "Основы построения защищенных компьютерных сетей" по направлению подготовки (специальности) 10.05.01 "Компьютерная безопасность" направленности (профилю) специализация N 6 "Информационно-аналитическая и техническая экспертиза компьютерных систем" ФГБОУ ВО «ЧелГУ»

стр. 7

допускает незначительные ошибки.

Неудовлетворительно/не зачтено/0 баллов - Работа не выполнена, либо обучающийся не может ответить на контрольные вопросы, не ориентируется в основных понятиях, излагает материал с трудом, с грубыми фактическими ошибками, либо отказывается от ответов на вопросы.

Критерии оценивания теоретического вопроса

Максимальный балл за ответ на один теоретический вопрос из билета — 15 баллов.

Максимальный балл за билет – 30 баллов.

Отлично/зачтено/15 баллов - Обучающийся отлично знает материал, умеет анализировать проблему и аргументировано изложить свою точку зрения с использованием точных терминов. Обучающийся практически не допускает ошибок.

Хорошо/зачтено/10-14 баллов - Обучающийся хорошо знает материал, умеет анализировать проблему и аргументировано изложить свою точку зрения. Обучающийся допускает незначительные ошибки.

Удовлетворительно/зачтено/5-9 баллов - Обучающийся знаком с материалом, но допускает фактические ошибки.

Неудовлетворительно/не зачтено/0-5 баллов - Обучающийся не знает основных положений вопроса, не ориентируется в основных понятиях, излагает материал с трудом, с грубыми фактическими ошибками, либо отказывается от ответов на вопросы.

При подведении итогов учитываются баллы за ответ на билет с двумя теоретическими вопросами, которые суммируются с текущими баллами, полученными за выполнение проверочной и лабораторных работ. Итого определяется 2 возможных результата промежуточной аттестации:

0-25 баллов - не зачтено;

26-45 баллов - зачтено.

## 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	Фефилов А. Д.	Методы и средства защиты информации в сетях: практическое пособие ( <a href="https://biblioclub.ru/index.php?page=book&amp;id=140796">https://biblioclub.ru/index.php?page=book&amp;id=140796</a> )	Москва : Лаборатория книги, 2011	ЭБС
Л1.2	Руденков Н. А., Пролетарский А. В., Смирнова Е. В., Суровов А. М.	Технологии защиты информации в компьютерных сетях: учебное пособие ( <a href="https://biblioclub.ru/index.php?page=book&amp;id=428820">https://biblioclub.ru/index.php?page=book&amp;id=428820</a> )	Москва : Национальный Открытый Университет «ИНТУИТ», 2016	ЭБС
Л1.3	Мэйволд Э.	Безопасность сетей: учебное пособие ( <a href="https://biblioclub.ru/index.php?page=book&amp;id=429035">https://biblioclub.ru/index.php?page=book&amp;id=429035</a> )	Москва : Национальный Открытый Университет «ИНТУИТ», 2016	ЭБС

#### 7.1.2. Дополнительная литература

	Авторы, составители	Заглавие	Издательство, год	Ресурс
Л2.1	Голиков А. М.	Защита информации в инфокоммуникационных системах и сетях: учебное пособие ( <a href="https://biblioclub.ru/index.php?page=book&amp;id=480637">https://biblioclub.ru/index.php?page=book&amp;id=480637</a> )	Томск : Томский государственный университет систем управления и радиоэлектроник и, 2015	ЭБС



	Авторы, составители	Заглавие	Издательство, год	Ресурс
Л2.2	Дятлов П. А.	Принципы построения и организация компьютерных сетей: учебное пособие ( <a href="https://biblioclub.ru/index.php?page=book&amp;id=698674">https://biblioclub.ru/index.php?page=book&amp;id=698674</a> )	Ростов-на-Дону, Таганрог : Южный федеральный университет, 2022	ЭБС
Л2.3	Пескова О.Ю., Басан Е.С.	Безопасность сетей ЭВМ: учебное пособие ( <a href="https://znanium.ru/catalog/document?id=455605">https://znanium.ru/catalog/document?id=455605</a> )	Ростов-на-Дону : Издательство Южного федерального университета (ЮФУ), 2024	ЭБС

### 7.3 Перечень информационных технологий

#### 7.3.1 Программное обеспечение

Adobe Reader

Notepad++

VirtualBox

Ubuntu Linux

#### 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. Консультант Плюс [Электронный ресурс] : справочно-правовая система : база данных / Регион. центр правовой информ. Информправо.
3. eLIBRARY.RU [Электронный ресурс] : научная электронная библиотека [научной периодики на русском языке ]. — Москва, [1999-]. - Доступ к полным текстам после регистрации из сети ЧелГУ. – URL: <http://elibrary.ru/defaultx.asp>.
4. Moodle [Электронный ресурс]: система дистанционного обучения : [база данных] / Челяб. гос. ун-т. – Челябинск, [б.г.]. – Доступ из сети ЧелГУ или, после регистрации из сети ун-та, из любой точки, имеющей доступ в интернет. – URL: <http://moodle.uio.csu.ru/login/index.php>.
5. Научная библиотека Челябинского государственного университета [Электронный ресурс] : [сайт] / Челяб. гос. ун-т. – Челябинск, [2001-]. – Режим доступа: <http://www.lib.csu.ru/>, свободный. – Загл. с экрана.
6. Интернет университет информационных технологий [Электронный ресурс]. – Электрон. дан. – Режим доступа : <http://www.intuit.ru/>

## 8. МАТЕРИАЛЬНО-ТЕХНИЧЕСКОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ (МОДУЛЯ)

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

Учебные аудитории укомплектованы специализированной мебелью и техническими средствами обучения: проектором, экраном, магнитно-маркерной доской, маркером; с возможностью демонстрации электронных презентаций при уровне освещения, достаточном для работы с конспектом.

Для проведения занятий лекционного типа имеется демонстрационное оборудование: проектор, экран.

Лабораторные занятия проходят в учебной лаборатории "Сетевой полигон" (ауд. 423, учебный корпус №1). Материально-техническое обеспечение приведено в паспорте лаборатории.

Помещения для самостоятельной работы обучающихся оснащены компьютерной техникой с подключением к сети «Интернет» и обеспечением доступа в электронную информационно-образовательную среду университета.

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

При изучении данной дисциплины используются лекционные, лабораторные занятия и самостоятельная работа студента. На лекционных занятиях преподаватель излагает основное содержание тем программы. Проработку лекционного материала студенту желательно проводить как после каждого занятия, так и по завершению темы. Это позволит связать воедино полученные сведения и составить цельную картину.



На лабораторных занятиях рассматриваются методы проектирования, эксплуатации и поиска неисправностей в конвергентных сетях. Рекомендуется перед каждым лабораторным занятием выполнить домашнее задание, что позволит лучше усвоить предыдущий материал, и изучить лекционный материал по предстоящей теме. Студенту желательно проявлять активное участие на лабораторных и лекционных занятиях, задавать вопросы, поскольку умение обосновывать свою точку зрения, нахождение компромиссного решения в этически выдержанной дискуссии не только важно для лучшего усвоения материала, но и ценится в реальной жизни.

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, форумы, электронная почта и др.).

Большую часть времени обучающиеся самостоятельно работают с учебно-методическими материалами. Студенты имеют возможность консультироваться с преподавателем по всем вопросам, возникающим в ходе самостоятельной работы посредством электронной почты, мессенджеров, социальных сетей и т.п.

Доступ обучающегося к учебным ресурсам в режиме отложенного времени, самостоятельной работы осуществляется через сеть Интернет в удобном для него месте, времени и темпе.

При обучении 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



МИНОБРНАУКИ РОССИИ  
Федеральное государственное бюджетное образовательное  
учреждение высшего образования  
«Челябинский государственный университет» (ФГБОУ ВО «ЧелГУ»)

Рабочая программа дисциплины "Основы построения защищенных компьютерных сетей" по направлению подготовки (специальности) 10.05.01 "Компьютерная безопасность" направленности (профилю) специализация N 6 "Информационно-аналитическая и техническая экспертиза компьютерных систем" ФГБОУ ВО «ЧелГУ»

стр. 10

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.

