

Документ подписан простой электронной подписью Информация о владельце: ФИО: Таскаев Сергей Валерьевич Должность: Ректор	МИНОБРНАУКИ РОССИИ Федеральное государственное бюджетное образовательное учреждение высшего образования «Челябинский государственный университет» (ФГБОУ ВО «ЧелГУ»)	
Дата подписания: 03.04.2025 17:01:09 Уникальный идентификатор направления (профилю) 04c19ed8bf98f3b6cb77a486b9a8788b8322323	Рабочая программа дисциплины "Защита IoT сетей" по направлению подготовки (специальности) "Компьютерная специализация N 1 "Анализ безопасности компьютерных систем": ФГБОУ ВО «ЧелГУ»	стр. 1



**УТВЕРЖДАЮ**

Проректор по учебной работе

В.Е. Федоров

2021 г.

**Рабочая программа дисциплины (модуля)\*  
Защита IoT сетей**

Направление подготовки (специальность)

10.05.01 Компьютерная безопасность

Направленность (профиль)

специализация № 1 "Анализ безопасности компьютерных систем"

Присваиваемая квалификация (степень)

специалист по защите информации

Форма обучения

очная

Год(ы) набора 2021

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

Челябинск 2021 г.

**Рабочая программа дисциплины (модуля) принята:**  
Ученым советом математического факультета

Протокол заседания № 13 от « 24 » 06 2021 г.

Председатель Ученого совета  
математического факультета  Е.А. Сбродова

Секретарь Ученого совета  
математического факультета  С.А. Никитина

**Рабочая программа дисциплины (модуля) одобрена и рекомендована кафедрой**  
компьютерной безопасности и прикладной алгебры.

Протокол заседания № 10 от « 04 » 06 2021 г.

Заведующий кафедрой  А.Н. Ручай

Авторы (составители):

Зав.кафедрой, канд.физ.-мат. наук, доцент  А.Н. Ручай

Старший преподаватель  Е.В. Фельдман

**Структура рабочей программы соответствует приказу ректора**  
**ФГБОУ ВО «ЧелГУ» от «05» декабря 2018 г. № 678-1**

## 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

Рабочая программа дисциплины "Защита IoT сетей" по направлению подготовки (специальности) "Компьютерная безопасность" направленности (профилю) специализация N 1 "Анализ безопасности компьютерных систем": ФГБОУ ВО «ЧелГУ»	стр. 4
---	--------

### 1. ЦЕЛИ ОСВОЕНИЯ ДИСЦИПЛИНЫ

Целью освоения дисциплины является получение систематизированных сведений, стандартов подходов к технической реализации концепции Интернета вещей (Internet of Things, IoT), а также смежных с ним инфокоммуникационных технологий (радиочастотной идентификации RFID, беспроводным сенсорным сетям WSN, межмашинным коммуникациям M2M).

Результаты обучения по дисциплине направлены на достижение индикаторов:

ПК-2.1. Обладает знаниями о принципах построения систем обнаружения компьютерных атак; о методах обработки данных мониторинга безопасности компьютерных систем и сетей; о порядке создания и структура отчета, создаваемого по результатам проверок; о способах обнаружения и нейтрализации последствий вторжений в компьютерные системы; о нормативных правовых актах в области защиты информации; о руководящих и методических документах уполномоченных федеральных органов исполнительной власти по защите информации.

ПК-2.2. Демонстрирует умения: формализовывать задачу управления безопасностью компьютерных систем; применять инструментальные средства проведения мониторинга защищенности компьютерных систем; Применять методы анализа защищенности компьютерных систем и сетей; структурировать аналитическую информацию для включения в отчет.

ПК-2.3. Имеет практический опыт (навыки): выполнение анализа защищенности компьютерных систем с использованием сканеров безопасности; выполнение анализа защищенности сетевых сервисов с использованием средств автоматического реагирования на попытки несанкционированного доступа к ресурсам компьютерных систем и сетей; составление отчетов по результатам проверок.

### 2. МЕСТО ДИСЦИПЛИНЫ В СТРУКТУРЕ ОПОП

Цикл (раздел) ОПОП:	Б1.В.ДВ.01.01
<b>2.1 Требования к предварительной подготовке обучающегося:</b>	
Компьютерные сети	
Основы построения защищенных компьютерных сетей	
<b>2.2 Дисциплины и практики, для которых освоение данной дисциплины (модуля) необходимо как предшествующее:</b>	
Знания полученные в этой дисциплине могут использоваться для прохождения практики и написания ВКР.	
Подготовка к процедуре защиты и защита выпускной квалификационной работы	

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

#### ПК-2: Способен проводить мониторинг защищенности компьютерных систем

##### Знать:

- общие положения интернета вещей;
- стандарты и протоколы передачи данных в IoT;
- практическую реализацию IoT;
- принципы построения систем обнаружения компьютерных атак;
- актуальные методы обработки данных мониторинга безопасности компьютерных систем и сетей;
- нормативные правовые акты в области защиты информации.

##### Уметь:

- решать задачу управления безопасностью компьютерных систем;
- применять инструментальные средства проведения мониторинга защищенности компьютерных систем;
- применять методы анализа защищенности компьютерных систем и сетей;
- структурировать аналитическую информацию для включения в отчет.

##### Владеть:

- навыками практической реализации IoT;
- навыками анализа защищенности компьютерных систем с использованием сканеров безопасности;
- навыками анализа защищенности сетевых сервисов с использованием средств автоматического реагирования на попытки несанкционированного доступа к ресурсам компьютерных систем и сетей;
- навыками составления отчетов по результатам проверок.

В результате освоения дисциплины обучающийся должен

<b>3.1</b>	<b>Знать:</b>
3.1.1	– стандарты подходов к технической реализации концепции Интернета вещей.
<b>3.2</b>	<b>Уметь:</b>

Рабочая программа дисциплины "Защита IoT сетей" по направлению подготовки (специальности) "Компьютерная безопасность" направленности (профилю) специализация N 1 "Анализ безопасности компьютерных систем": ФГБОУ ВО «ЧелГУ»		стр. 5
3.2.1	– применять инструментальные средства проведения мониторинга защищенности компьютерных систем.	
<b>3.3 Владеть:</b>		
3.3.1	– практической реализации IoT.	

#### 4. ОБЪЕМ ДИСЦИПЛИНЫ (МОДУЛЯ)

Общая трудоемкость	<b>3 ЗЕТ</b>
Часов по учебному плану : 108 в том числе : аудиторные занятия : 54 самостоятельная работа : 54 :	Виды контроля в семестрах:  зачеты 8

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

Код занятия	Наименование разделов и тем /вид занятия/	Семестр / Курс	Часов	Литература
<b>Раздел 1. Общие положения интернета вещей.</b>				
1.1	Введение. Общие положения интернета вещей. Базовые принципы IoT. Стандартизация IoT . Архитектура IoT. Веб вещей WoT. Интернет нано-вещей. Когнитивный Интернет вещей CIoT. Способы взаимодействия с интернет-вещами. Зрелость концепции IoT и составляющих ее технологий. /Лек/	8	2	Л1.1 Л1.2 Л1.3Л2.1 Л2.2
1.2	Взаимодействие IoT с перспективными инфокоммуникационными технологиями. Большие данные (Big Data). Облачные вычисления (Cloud Computing). Повсеместная компьютеризация (Ubiquitous Computing). Направления практического применения IoT. Планы и прогнозы внедрения IoT. Проблемы внедрения IoT /Лек/	8	2	Л1.1 Л1.2 Л1.3Л2.1 Л2.2
<b>Раздел 2. Радиочастотная дентификация RFID</b>				
2.1	Общие сведения о радиочастотной идентификации RFID. Метки RFID. Считывающие устройства RFID. Стандартизация технологии RFID. Области применения RFID-технологий. /Лек/	8	2	Л1.1 Л1.2 Л1.3Л2.1 Л2.2
2.2	Радиочастотная идентификация RFID. Метки RFID. Считывающие устройства RFID. Стандартизация технологии RFID. /Лаб/	8	6	Л1.1 Л1.2 Л1.3Л2.1 Л2.2
2.3	Современное состояние и перспективы развития технологии RFID /Ср/	8	10	Л1.1 Л1.2 Л1.3Л2.1 Л2.2
<b>Раздел 3. Беспроводные сенсорные сети WSN</b>				
3.1	Основные понятия и принципы сенсорных сетей. Базовая архитектура сенсорной сети. Узлы беспроводной сенсорной сети. Способы передачи данных в БСС. Протоколы и технологии передачи данных в БСС. Мобильные БСС. Сопряжение БСС с сетями общего пользования /Лек/	8	2	Л1.1 Л1.2 Л1.3Л2.1 Л2.2
3.2	Базовая архитектура сенсорной сети. /Лаб/	8	4	Л1.1 Л1.2 Л1.3Л2.1 Л2.2
3.3	Типовые архитектуры и топологии БСС /Лаб/	8	4	Л1.1 Л1.2 Л1.3Л2.1 Л2.2
3.4	Протоколы маршрутизации в БСС /Лаб/	8	2	Л1.1 Л1.2 Л1.3Л2.1 Л2.2

Рабочая программа дисциплины "Защита IoT сетей" по направлению подготовки (специальности) "Компьютерная безопасность" направленности (профилю) специализация N 1 "Анализ безопасности компьютерных систем": ФГБОУ ВО «ЧелГУ»				стр. 6
3.5	Проблемы реализации БСС. Проблема энергопотребления. Проблема самоуправления. Проблема беспроводного соединения. Проблема децентрализованного управления. Проблема конструкции. Проблема безопасности. /Лаб/	8	4	Л1.1 Л1.2 Л1.3Л2.1 Л2.2
3.6	4 БСС и Интернет вещей /Ср/	8	10	Л1.1 Л1.2 Л1.3Л2.1 Л2.2
<b>Раздел 4. Межмашинные коммуникации M2M</b>				
4.1	Общие принципы M2M. Стандартизация M2M. Коммуникации малого радиуса действия NFC. Промышленные сети для реализации M2M. Современное состояние и перспективы применения M2M. /Лек/	8	2	Л1.1 Л1.2 Л1.3Л2.1 Л2.2
<b>Раздел 5. Стандарты и протоколы передачи данных в IoT</b>				
5.1	Классификация технологий передачи данных в IoT. Стандарт IEEE Std 802.15.4. Стандарт ZigBee. Стандарт 6LoWPAN. Стандарты WirelessHART и ISA100.11a. Стандарт Z-Wave. Стандарт Bluetooth Low Energy. Семейство стандартов IEEE 802.11. Протокол MQTT /Лек/	8	4	Л1.1 Л1.2 Л1.3Л2.1 Л2.2
5.2	Стандарты и протоколы передачи данных в IoT /Ср/	8	20	Л1.1 Л1.2 Л1.3Л2.1 Л2.2
<b>Раздел 6. Практическая реализация IoT</b>				
6.1	Практическая реализация IoT. «Умная планета». «Умный город». «Умный дом». «Умная энергия». «Умный транспорт». «Умное производство». «Умная медицина». «Умная жизнь». /Лек/	8	4	Л1.1 Л1.2 Л1.3Л2.1 Л2.2
6.2	Практическая реализация IoT. /Лаб/	8	16	Л1.1 Л1.2 Л1.3Л2.1 Л2.2
6.3	Практическая реализация IoT. /Ср/	8	14	Л1.1 Л1.2 Л1.3Л2.1 Л2.2

## 6. ФОНД ОЦЕНОЧНЫХ СРЕДСТВ

### 6.1. Перечень видов оценочных средств

аудиторные задания  
зачетные задания  
зачет

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

Аудиторные задания:  
Загрузка и выгрузка прошивки из устройств  
Написание прошивки для устройств  
Зачетные задания:  
Загрузка и выгрузка прошивки из устройств  
Написание прошивки для устройств  
Зачет:  
описание уязвимостей IoT сетей  
самые актуальные уязвимости IoT сетей  
нахождение уязвимостей в прошивках IoT сетей

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

Аудиторные задания:  
 Написание эксплойтов для прошивок IoT устройств  
 Написание прошивки для передачи информации по каналам связи  
 Зачетные задания:  
 Выявление уязвимостей в прошивке IoT устройств  
 Зачет:  
 Провести атаку на IoT сеть  
 Провести сканирование IoT сети и сформировать вектор атаки

#### 6.4. Критерии оценивания

Полнота и правильность ответа

Порядок проведения промежуточной аттестации  
 В течении семестра на практических занятиях проводится регулярный устный опрос. По учебному плану предусмотрены 18 академических часов, или 9 практических занятий.  
 Набранные баллы на практических занятиях являются допуском к зачету.  
 Максимальный балл за один устный опрос – 10 баллов.  
 Максимальный балл за все устные опросы – 90 баллов.  
 Более 50 баллов, набранных в семестре, – допуск к промежуточной аттестации, менее 50 – недопуск.

Сводная таблица рейтинга успеваемости  
 № Перечень контрольных мероприятий в семестре Максимальное кол-во баллов

1 Устный опрос на практических занятиях	9x10=90
Итого:	
Допуск к промежуточной аттестации	Более 50
Недопуск к промежуточной аттестации	Менее 50
2 Зачет	100
Итого	100

Критерии оценивания устного опроса на практических занятиях  
 Максимальный балл за ответ на теоретический вопрос – 10 баллов.  
 Отлично/зачтено/9-10 баллов - Обучающийся отлично знает материал, умеет анализировать проблему и аргументировано изложить свою точку зрения, грамотно изъясняется с использованием точных терминов. Обучающийся практически не допускает ошибок.  
 Хорошо/зачтено/7-8 баллов - Обучающийся хорошо знает материал, умеет анализировать проблему и аргументировано изложить свою точку зрения, грамотно изъясняется с использованием точных терминов. Обучающийся допускает незначительные ошибки.  
 Удовлетворительно/зачтено/5-6 баллов - Обучающийся знаком с материалом. Обучающийся допускает фактические ошибки.  
 Неудовлетворительно/не зачтено/0-4 балла - 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.

Критерии оценивания теста на зачете  
 Тест формируется в системе электронного обучения MOODLE.  
 Максимальный балл за тест – 100 баллов.  
 Отлично/зачтено/91-100 баллов  
 Хорошо/зачтено/70-90 баллов  
 Удовлетворительно/зачтено/50-69 баллов  
 Неудовлетворительно/не зачтено/0-49 баллов

При подведении итогов учитываются результаты текущей аттестации. Полученные за текущую аттестацию баллы суммируются с баллами, полученными за каждый этап при прохождении промежуточной аттестации:  
 0-49 баллов - не зачтено;  
 50-100 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
---------------------	----------	-------------------	--------

Рабочая программа дисциплины "Защита IoT сетей" по направлению подготовки (специальности) "Компьютерная безопасность" направленности (профилю) специализация N 1 "Анализ безопасности компьютерных систем": ФГБОУ ВО «ЧелГУ»				стр. 8
	Авторы, составители	Заглавие	Издательство, год	Ресурс
Л1.1	Грингард С.	Интернет вещей: Будущее уже здесь ( <a href="http://znanium.com/catalog/document?id=333356">http://znanium.com/catalog/document?id=333356</a> )	Москва : ООО "Альпина Паблишер", 2016	ЭБС
Л1.2	Ли П.	Архитектура интернета вещей ( <a href="https://e.lanbook.com/book/112923">https://e.lanbook.com/book/112923</a> )	Москва : ДМК Пресс, 2019	ЭБС
Л1.3	Зараменских Е.П., Артемьев И.Е.	Интернет вещей. Исследования и область применения: монография ( <a href="http://znanium.com/catalog/document?id=359780">http://znanium.com/catalog/document?id=359780</a> )	Москва : ООО "Научно-издательский центр ИНФРА-М", 2020	ЭБС
<b>7.1.2. Дополнительная литература</b>				
	Авторы, составители	Заглавие	Издательство, год	Ресурс
Л2.1	Дубков И. С., Сташевский П. С., Яковина И. Н.	Решение практических задач на базе технологии интернета вещей: учебное пособие ( <a href="https://biblioclub.ru/index.php?page=book&amp;id=576635">https://biblioclub.ru/index.php?page=book&amp;id=576635</a> )	Новосибирск : Новосибирский государственный технический университет, 2017	ЭБС
Л2.2	Филимонова А. А.	Разработка ПО, обеспечивающего безопасность помещения с помощью «умных вещей»: студенческая научная работа ( <a href="https://biblioclub.ru/index.php?page=book&amp;id=596766">https://biblioclub.ru/index.php?page=book&amp;id=596766</a> )	Благовещенск : б.и., 2020	ЭБС
<b>7.2. Перечень ресурсов информационно-телекоммуникационной сети "Интернет"</b>				
Э1	Официальный интернет-портал правовой информации. Государственная система правовой информации <a href="http://pravo.gov.ru">http://pravo.gov.ru</a> Раздел «Официальное опубликование правовых актов» в электронном виде» <a href="http://publication.pravo.gov.ru/">http://publication.pravo.gov.ru/</a> <a href="http://publication.pravo.gov.ru/">http://publication.pravo.gov.ru/</a>			
<b>7.3 Перечень информационных технологий</b>				
<b>7.3.1 Программное обеспечение</b>				
LMS Moodle				
MS Office365				
Python				
VirtualBox				
Visual Studio				
Adobe Connect Acrobat				
<b>7.3.2 Профессиональные базы данных и информационно-справочные системы</b>				
Архив крупнейших научных зарубежных журналов (Annual Reviews, Cambridge University Press, Nature, Oxford University Press, Royal Society of Chemistry, SAGE, Science, Taylor&Francis, The Institute of Physics, Wiley) ( <a href="https://arch.neicon.ru/xmlui/">https://arch.neicon.ru/xmlui/</a> ) Архив научных журналов : [сайт] / Национальный электронноинформационный консорциум (НП НЭИКОН). – URL: <a href="http://arch.neicon.ru/xmlui/">http://arch.neicon.ru/xmlui/</a> . – Режим доступа: доступ только из сети университета. – Текст : электронный.				

## 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.

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)

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, 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

## 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 голо информационных технологий, предоставляемых Ресурсным учебно-методическим центром по обучению инвалидов и лиц с ограниченными возможностями здоровья ЧелГУ по запросу обучающегося.

1. Мобильные специальные технические средства для лиц с нарушениями зрения: портативный компьютер с вводом/выводом шрифтом Брайля с синтезатором речи «EIBraile-W14J G2»; ноутбуки с программой экранного доступа NVDA; электронные увеличители для удаленного просмотра; видеоувеличители портативные; тифлоплеер; цифровые диктофоны.

2. Мобильные специальные технические средства для лиц с нарушениями слуха: система свободного звукового поля со встроенной совместимостью с FM-устройствами; радиоклассы «Сонет-PCM» с передатчиком, заушным индуктором и индукционной петлей; система информационная для слабослышащих переносная «Исток» А2 со встроенным плеером – звуковым информатором; документ-камера; программируемые слуховые аппараты индивидуального пользования.

3. Ассистивные информационные технологии: программное обеспечение экранного доступа с синтезом речи NVDA; программы экранного увеличения; программы речевого синтеза для компьютеров и ноутбуков; программы речевого синтеза для мобильных устройств; экранная клавиатура; экранная лупа.

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

В учебные аудитории обеспечивается беспрепятственный доступ для обучающихся инвалидов и обучающихся 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 к электронным источникам, представленным в форме электронного документа в фонде научной библиотеки ЧелГУ или электронно-библиотечных системах, с помощью специальных технических и программных средств (рабочее место для незрячего пользователя с программным обеспечением экранного доступа с синтезом речи NVDA, рабочее место с компьютерным роллером и клавиатурой Clevy с большими кнопками и с разделяющей клавиши накладкой).

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

Для лиц с нарушениями зрения:

- в печатной форме увеличенным шрифтом,
- в форме электронного документа,
- в форме аудиофайла,
- в печатной форме шрифтом Брайля.

Для лиц с нарушениями слуха:

- в печатной форме,
- в форме электронного документа.

Для лиц с нарушениями опорно-двигательного аппарата:

- в печатной форме,
- в форме электронного документа,
- в форме аудиофайла.

Данный перечень может быть конкретизирован в зависимости от контингента обучающихся.

Для инвалидов и лиц с ограниченными возможностями здоровья освоение дисциплины может быть частично или полностью осуществлено с использованием дистанционных образовательных технологий (Moodle, Adobe Connect Pro и пр.).

В освоении дисциплины инвалидами и лицами с ограниченными возможностями здоровья используется индивидуальная работа. Под индивидуальной работой подразумевается две формы взаимодействия с преподавателем: индивидуальная учебная работа (консультации), т.е. дополнительное разъяснение учебного материала и углубленное изучение материала с теми обучающимися, которые в этом заинтересованы, и индивидуальная воспитательная работа. Индивидуальные консультации направлены на индивидуализацию обучения и установлению воспитательного контакта между преподавателем и обучающимся инвалидом или обучающимся с ограниченными возможностями здоровья.

При проведении процедуры оценивания результатов обучения инвалидов и лиц с ограниченными возможностями здоровья по дисциплине обеспечивается выполнение следующих дополнительных требований в зависимости от индивидуальных особенностей, обучающихся:

Рабочая программа дисциплины "Защита IoT сетей" по направлению подготовки (специальности) "Компьютерная безопасность" направленности (профилю) специализация N 1 "Анализ безопасности компьютерных систем": ФГБОУ ВО «ЧелГУ»	стр. 10
<p>а) инструкция по порядку проведения процедуры оценивания предоставляется в доступной форме (устно, в письменной форме, в письменной форме шрифтом Брайля, устно с использованием услуг сурдопереводчика);</p> <p>б) доступная форма предоставления заданий оценочных средств (в печатной форме, в печатной форме увеличенным шрифтом, в печатной форме шрифтом Брайля, в форме электронного документа, задания зачитываются ассистентом, задания предоставляются с использованием сурдоперевода);</p> <p>в) доступная форма предоставления ответов на задания (письменно на бумаге, набор ответов на компьютере, письменно шрифтом Брайля, с использованием услуг ассистента, устно).</p> <p>При проведении процедуры оценивания результатов обучения инвалидов и лиц с ограниченными возможностями здоровья предусматривается использование технических средств, необходимых им в связи с их индивидуальными особенностями. Эти средства могут быть предоставлены ЧелГУ или могут использоваться собственные технические средства. 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.</p> <p>Проведение процедуры оценивания результатов обучения инвалидов и лиц с ограниченными возможностями здоровья допускается с использованием дистанционных образовательных технологий.</p>	