УТВЕРЖДАЮ
Проректор по учебной работе
_____________ В.Е. Федоров
«25» 06 2021 г.

Рабочая программа дисциплины (модуля)*
Организационное и правовое обеспечение информационной безопасности

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

Автор (составитель):
Зав.кафедрой, канд.физ.-мат. наук, доцент _____ А.Н. Ручай

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

Содержание

1. ЦЕЛИ ОСВОЕНИЯ ДИСЦИПЛИНЫ

Целью освоения дисциплины является получение студентами представления о правовой организации защиты информации, предъявляемых требований к организациям в области защиты информации и получение навыков применения организационных и технических мер защиты информации.

Результаты обучения по дисциплине направлены на достижение индикаторов:

ОПК-5.1 Знает основы: российской правовой системы и законодательства, правового статуса личности, организации и деятельности органов государственной власти в Российской Федерации; основные понятия и характеристику основных отраслей права применяемых в профессиональной деятельности организации; основы законодательства Российской Федерации, нормативные правовые акты, нормативные и методические документы в области информационной безопасности и защиты информации, правовые основы организации защиты государственной тайны и конфиденциальной информации, правовую характеристику преступлений в сфере компьютерной информации и меры правовой и дисциплинарной ответственности за разглашение защищаемой информации; правовые основы организации защиты персональных данных и охраны результатов интеллектуальной деятельности.

ОПК-5.2 Умеет обосновывать решения, связанные с реализацией правовых норм по защите информации в пределах должностных обязанностей,предпринимать необходимые меры по восстановлению нарушенных прав; анализировать и разрабатывать проекты локальных правовых актов, инструкций, регламентов и организационно-распорядительных документов, регламентирующих работу по обеспечению информационной безопасности в организации; формулировать основные требования при лицензировании деятельности в области защиты информации, сертификации и аттестации по требованиям безопасности информации; формулировать основные требования информационной безопасности при эксплуатации компьютерной системы; формулировать основные требования по защитеконфиденциальной информации, персональных данных и охране результатов интеллектуальной деятельности в организации.

ОПК-6.1 Знает систему нормативных правовых актов и стандартов по лицензированию в области обеспечения защиты государственной тайны, технической защиты конфиденциальной информации, по аттестации объектов информатизации и сертификации средств защиты информации; задачи органов защиты государственной тайны и служб защиты информации на предприятиях; систему организационных мер, направленных на защиту информации ограниченного доступа; нормативные, руководящие и методические документы уполномоченных федеральных органов исполнительной власти по защите информации ограниченного доступа; основные угрозы безопасности информации и модели нарушителя компьютерных систем.

ОПК-6.2 Умеет разрабатывать модели угроз и модели нарушителя компьютерных систем; разрабатывать проекты инструкций, регламентов, положений и приказов, регламентирующих защиту информации ограниченного доступа в организации; определить политику контроля доступа работников к информации ограниченного доступа; формулировать основные требования, предъявляемые к физической защите объекта и пропускному режиму в организации; применять отечественные и зарубежные стандарты в области компьютерной безопасности для проектирования, разработки и оценивания защищенности компьютерной системы.

2. МЕСТО ДИСЦИПЛИНЫ В СТРУКТУРЕ ОПОП

Цикл (раздел) ОПОП:	Б1.О.22

2.1 Требования к предварительной подготовке обучающегося:

Дисциплина базируется на знаниях, полученных при изучении таких дисциплин как: "Правоведение" и "Основы информационной безопасности"

Правоведение

Основы информационной безопасности

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

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

ОПК-5: Способен применять нормативные правовые акты, нормативные и методические документы, регламентирующие деятельность по защите информации;

Знать:

– источники и классификацию угроз информационной безопасности;
– требования по защите информации при использовании СКЗИ;
– основные средства и способы обеспечения информационной безопасности, принципы построения систем защиты информации.

Уметь:

– классифицировать защищаемую информацию по видам тайны и степеням конфиденциальности;
– классифицировать и оценивать угрозы информационной безопасности для объекта информатизации;
– разрабатывать требования к системе защиты информации.

Владеть:

– навыками работы с нормативными правовыми актами в области информационной безопасности;
– навыками применения современной нормативной базы для построения системы организационных и программно-технических мер по выявлению и нейтрализации угроз безопасности компьютерных систем.

ОПК-6: Способен при решении профессиональных задач организовывать защиту информации ограниченного доступа в компьютерных системах и сетях в соответствии с нормативными правовыми актами и нормативными методическими документами Федеральной службы безопасности Российской Федерации, Федеральной службы по техническому и экспортному контролю;

Знать:

– нормативные правовые акты в области защиты информации.

Уметь:

– использовать методы и средства обеспечения информационной безопасности с целью предотвращения несанкционированного доступа, злоумышленной модификации или утраты информации, составляющей государственную тайну и иной служебной информации.

Владеть:

– навыками обеспечения использования правовых актов в своей профессиональной деятельности.

В результате освоения дисциплины обучающийся должен

3.1	**Знать:**
3.1.1	– основное законодательство в сфере защиты информации;
3.1.2	– основные методы защиты информации;
3.1.3	– требование регулирующих органов в сфере защиты информации.
3.2	**Уметь:**
3.2.1	– разрабатывать методические документы по защите информации;
3.2.2	– подготавливать кабинеты и автоматизированные рабочие места к проверочным мероприятиям;
3.2.3	– выдвигать требования для получения лицензий в области защиты информации.
3.3	**Владеть:**
3.3.1	– внедрять разработанные методические документы;
3.3.2	– настраивать автоматизированные рабочие места в соответствии с требованиями по защите информации;
3.3.3	– подбирать оборудование и программы необходимые для получения лицензий в области защиты информации.

4. ОБЪЕМ ДИСЦИПЛИНЫ (МОДУЛЯ)

Общая трудоемкость	**3 ЗЕТ**
Часов по учебному плану : 108 в том числе : аудиторные занятия : 54 самостоятельная работа : 54 :	Виды контроля в семестрах: зачеты 10

5. СТРУКТУРА И СОДЕРЖАНИЕ ДИСЦИПЛИНЫ (МОДУЛЯ)

Код занятия	Наименование разделов и тем /вид занятия/	Семестр / Курс	Часов	Литература
	Раздел 1. 1 Понятие, предмет и содержание курса. Организационные источники и каналы утечки			
1.1	Понятие, предмет и содержание курса. Организационные источники и каналы утечки /Лек/	10	2	Л1.1 Л1.2 Л1.3Л2.1 Л2.2
1.2	Проработка лекционного материала /Ср/	10	6	Л1.1 Л1.2 Л1.3Л2.1 Л2.2
	Раздел 2. 2. Порядок засекречивания и рассекречивания конфиденциальных сведений, документов и изделий			
2.1	Порядок засекречивания и рассекречивания конфиденциальных сведений, документов и изделий /Лек/	10	2	Л1.1 Л1.2 Л1.3Л2.1 Л2.2

2.2	Порядок засекречивания и рассекречивания конфиденциальных сведений, документов и изделий /Пр/	10	2	Л1.1 Л1.2 Л1.3Л2.1 Л2.2
2.3	Проработка лекционного материала /Ср/	10	6	Л1.1 Л1.2 Л1.3Л2.1 Л2.2
	Раздел 3. 3. Подбор сотрудников на должности, связанные с работой с конфиденциальной информацией, и текущая работа с ним.			
3.1	Подбор сотрудников на должности, связанные с работой с конфиденциальной информацией, и текущая работа с ним. /Лек/	10	2	Л1.1 Л1.2 Л1.3Л2.1 Л2.2
3.2	Подбор сотрудников на должности, связанные с работой с конфиденциальной информацией, и текущая работа с ним. /Пр/	10	2	Л1.1 Л1.2 Л1.3Л2.1 Л2.2
3.3	Проработка лекционного материала /Ср/	10	6	Л1.1 Л1.2 Л1.3Л2.1 Л2.2
	Раздел 4. 4. Допуск и доступ к государственной, служебной тайнам и персональным данным сотрудников			
4.1	Допуск и доступ к государственной, служебной тайнам и персональным данным сотрудников /Лек/	10	4	Л1.1 Л1.2 Л1.3Л2.1 Л2.2
4.2	Допуск и доступ к государственной, служебной тайнам и персональным данным сотрудников /Пр/	10	2	Л1.1 Л1.2 Л1.3Л2.1 Л2.2
4.3	Допуск и доступ к государственной, служебной тайнам и персональным данным сотрудников. Проработка лекционного материала /Ср/	10	6	Л1.1 Л1.2 Л1.3Л2.1 Л2.2
	Раздел 5. 5 Организация служебного расследования по фактам разглашения и утечки конфиденциальной информации			
5.1	Организация служебного расследования по фактам разглашения и утечки конфиденциальной информации /Лек/	10	4	Л1.1 Л1.2 Л1.3Л2.1 Л2.2
5.2	Организация служебного расследования по фактам разглашения и утечки конфиденциальной информации /Пр/	10	2	Л1.1 Л1.2 Л1.3Л2.1 Л2.2
5.3	Организация служебного расследования по фактам разглашения и утечки конфиденциальной информации. Проработка лекционного материала /Ср/	10	6	Л1.1 Л1.2 Л1.3Л2.1 Л2.2
	Раздел 6. 6 Организация охраны территории, зданий, помещений и сотрудников. Организация пропускного и внутриобъектового режимов			
6.1	Организация охраны территории, зданий, помещений и сотрудников. Организация пропускного и внутриобъектового режимов /Лек/	10	4	Л1.1 Л1.2 Л1.3Л2.1 Л2.2
6.2	Организация охраны территории, зданий, помещений и сотрудников. Организация пропускного и внутриобъектового режимов /Пр/	10	2	Л1.1 Л1.2 Л1.3Л2.1 Л2.2
6.3	Организация охраны территории, зданий, помещений и сотрудников. Организация пропускного и внутриобъектового режимов. Проработка лекционного материала /Ср/	10	6	Л1.1 Л1.2 Л1.3Л2.1 Л2.2
	Раздел 7. 7 Требования к помещениям и хранилищам, в которых ведутся закрытые работы и хранятся конфиденциальные документы и изделия			
7.1	Требования к помещениям и хранилищам, в которых ведутся закрытые работы и хранятся конфиденциальные документы и изделия /Лек/	10	6	Л1.1 Л1.2 Л1.3Л2.1 Л2.2
7.2	Требования к помещениям и хранилищам, в которых ведутся закрытые работы и хранятся конфиденциальные документы и изделия /Пр/	10	2	Л1.1 Л1.2 Л1.3Л2.1 Л2.2
7.3	Требования к помещениям и хранилищам, в которых ведутся закрытые работы и хранятся конфиденциальные документы и изделия. Проработка лекционного материала /Ср/	10	6	Л1.1 Л1.2 Л1.3Л2.1 Л2.2
	Раздел 8. 8 Аналитическая работа как основа управления системой организационной защиты информации			
8.1	Аналитическая работа как основа управления системой организационной защиты информации /Лек/	10	6	Л1.1 Л1.2 Л1.3Л2.1 Л2.2
8.2	Аналитическая работа как основа управления системой организационной защиты информации /Пр/	10	2	Л1.1 Л1.2 Л1.3Л2.1 Л2.2

8.3	Аналитическая работа как основа управления системой организационной защиты информации. Проработка лекционного материала /Ср/	10	6	Л1.1 Л1.2 Л1.3Л2.1 Л2.2
	Раздел 9. 9 Планирование процессов организационной защиты информации			
9.1	Планирование процессов организационной защиты информации /Лек/	10	6	Л1.1 Л1.2 Л1.3Л2.1 Л2.2
9.2	Планирование процессов организационной защиты информации /Пр/	10	4	Л1.1 Л1.2 Л1.3Л2.1 Л2.2
9.3	Планирование процессов организационной защиты информации. Проработка лекционного материала /Ср/	10	6	Л1.1 Л1.2 Л1.3Л2.1 Л2.2

6. ФОНД ОЦЕНОЧНЫХ СРЕДСТВ

6.1. Перечень видов оценочных средств

Ответы на занятиях
Промежуточные тесты
Итоговый тест

6.2. Типовые контрольные задания и иные материалы для текущей аттестации

Ответы на занятиях (Написать вопросы)
Промежуточные тесты (Написать)

6.3. Типовые контрольные вопросы и задания для промежуточной аттестации

Теоретические вопросы к зачету
1) понятие КИИ
2) понятие государственной тайны
3) понятие персональных данных
4) требования к защите государственной тайны
5) порядок доступа к государственной тайне
6) каналы утечки информации
7) понятие государственной информационной системы
8) понятие автоматизированной системы
9) требования по защите государственных информационных систем
10) требования по защите автоматизированных систем
11) требования по организации работы с СКЗИ
12) аттестация информационных систем

Итоговый тест
1) выберите правильное определения персональных данных
2) выберите правильное определение государственной тайны
3) что не входит в понятие персональных данных
4) в каких случаях аттестация обязательна
5) какие лицензии в контексте защиты информации выдает ФСБ России
6) какие лицензии в контексте защиты информации выдает ФСТЭК России

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
Л1.1	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
Л1.2	Партыка Т. Л., Попов И.И.	Информационная безопасность: учебное пособие (http://znanium.com/catalog/document?id=364624)	Москва : Издательство "ФОРУМ", 2021	ЭБС
Л1.3	Полякова Т. А., Чубукова С. Г., Ниесов В. А., Стрельцов А. А.	Организационное и правовое обеспечение информационной безопасности: учебник и практикум для вузов (https://urait.ru/bcode/469235)	Москва : Юрайт, 2021	ЭБС

7.1.2. Дополнительная литература

	Авторы, составители	Заглавие	Издательство, год	Ресурс
Л2.1	Кармановский Н. С., Михайличенко О. В., Прохожев Н. Н.	Организационно-правовое и методическое обеспечение информационной безопасности (https://e.lanbook.com/book/91449)	Санкт- Петербург : НИУ ИТМО, 2016	ЭБС
Л2.2	Баранова Е.К., Бабаш А.В.	Информационная безопасность и защита информации: учебное пособие (http://znanium.com/catalog/document?id=364911)	Москва : Издательский Центр РИОР, 2021	ЭБС

7.2. Перечень ресурсов информационно-телекоммуникационной сети "Интернет"

Э1	Официальный интернет-портал правовой информации. Государственная система правовой информации http://pravo.gov.ru Раздел «Официальное опубликование правовых актов» в электронном виде» http://publication.pravo.gov.ru/ http://publication.pravo.gov.ru/

7.3 Перечень информационных технологий

7.3.1 Программное обеспечение

LMS Moodle

MS Office365

Adobe Reader

7.3.2 Профессиональные базы данных и информационно-справочные системы

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

2. Консультант Плюс [Электронный ресурс] : справочно-правовая система : база данных / Регион.центр правовой информ. Информправо.

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)

При изучении данной дисциплины используются лекционные, практические 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 практических занятиях рассматриваются основные понятия, принципы, уровни и угрозы информационной безопасности. Рекомендуется перед каждым практическим занятием выполнить домашнее задание, что позволить лучше усвоить предыдущий материал, и изучить лекционный материал по предстоящей теме. Студенту желательно проявлять активное участие на практических 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, видеохостинг YouYube, 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 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 «ElBraile-W14J G2»; ноутбуки с программной 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-РСМ» 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:

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);

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);

в) доступная форма предоставления 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 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.

Проведение процедуры оценивания результатов обучения инвалидов и лиц с ограниченными возможностями здоровья допускается с использованием дистанционных образовательных технологий.