

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: 02.04.2021 17:01:30 Уникальный идентификатор: 04c19ed88fb98f3b6cb77a486b9a8788b8322323	Рабочая программа дисциплины "Защита web-приложений" по направлению подготовки (специальности) "Компьютерная безопасность" направленности (профилю) 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 web-приложений**

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
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 web-приложений" 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:	
обучение студентов принципам обнаружения уязвимостей в web-приложениях и методам защиты от них.	
Результаты обучения по дисциплине направлены на достижение индикаторов:	
УК-4.1. Обладает знаниями особенностей и правил личной и профессиональной устной и письменной коммуникации, в том числе на иностранном(ых) языке(ах).	
УК-4.2. Демонстрирует умение применять современные коммуникативные технологии для академического и профессионального взаимодействия в ситуации устной и письменной коммуникации, в том числе на иностранном (ых) языке(ах)	
УК-4.3. Имеет навыки академического и профессионального взаимодействия, в том числе на иностранном(ых) языке (ах).	
ПК-4.1. Обладает знаниями о формировании политик безопасности компьютерных систем; о разработке технических заданий на создание средств защиты информации; об определении угроз безопасности информации, реализация которых может привести к нарушению безопасности информации в компьютерной системе и сети; о требованиях к защите информации компьютерной системы; о разработке руководящих документов по защите информации.	
ПК-4.2. Демонстрирует умения: анализировать компьютерную систему с целью определения необходимого уровня защищенности и доверия; разрабатывать профили защиты компьютерных систем; формулировать задания по безопасности компьютерных систем; выполнять анализ безопасности компьютерных систем и разрабатывать рекомендации по эксплуатации системы защиты информации; формировать политики безопасности компьютерных систем и сетей.	
ПК-4.3. Имеет практический опыт (навыки): использования средств защиты информации; использования нормативные правовые акты в области защиты информации; разработки руководящих документов по защите информации.	

2. МЕСТО ДИСЦИПЛИНЫ В СТРУКТУРЕ ОПОП	
Цикл (раздел) ОПОП:	К.М.03.07
2.1 Требования к предварительной подготовке обучающегося:	
Информатика	
Аппаратные средства вычислительной техники	
Алгебра	
Модели безопасности компьютерных систем	
Методы программирования	
Компьютерные сети	
Web-программирование	
Беспроводные сети	
2.2 Дисциплины и практики, для которых освоение данной дисциплины (модуля) необходимо как предшествующее:	
Подготовка к процедуре защиты и защита выпускной квалификационной работы	

3. КОМПЕТЕНЦИИ ОБУЧАЮЩЕГОСЯ, ФОРМИРУЕМЫЕ В РЕЗУЛЬТАТЕ ОСВОЕНИЯ ДИСЦИПЛИНЫ (МОДУЛЯ)	
УК-4: Способен применять современные коммуникативные технологии, в том числе на иностранном(ых) языке(ах), для академического и профессионального взаимодействия	
Знать:	
– основные термины и речевые обороты, употребляющиеся в сфере компьютерных технологий.	
Уметь:	
– составлять тексты и сообщения с описанием технологических и программных характеристик разрабатываемых продуктов.	
Владеть:	
– иметь навыки вербальной коммуникации на техническом иностранном языке.	
ПК-4: Способен разрабатывать требования и рекомендации к системам защиты информации в web- приложениях	
Знать:	
– основы политики безопасности компьютерных систем;	

Рабочая программа дисциплины "Защита web-приложений" по направлению подготовки (специальности) "Компьютерная безопасность" направленности (профилю) специализация N 1 "Анализ безопасности компьютерных систем": ФГБОУ ВО «ЧелГУ»	стр. 5
<ul style="list-style-type: none"> – алгоритмы разработки технических заданий на создание средств защиты информации; – определении угроз безопасности информации, реализация которых может привести к нарушению безопасности информации в компьютерной системе и сети; – требования к защите информации компьютерной системы; – алгоритмы разработки руководящих документов по защите информации. 	
Уметь:	
<ul style="list-style-type: none"> – анализировать компьютерную систему с целью определения необходимого уровня защищенности и доверия; – разрабатывать профили защиты компьютерных систем; – формулировать задания по безопасности компьютерных систем; – выполнять анализ безопасности компьютерных систем и разрабатывать рекомендации по эксплуатации системы защиты информации; – формировать политики безопасности компьютерных систем и сетей. 	
Владеть:	
<ul style="list-style-type: none"> – навыками использования средств защиты информации; – навыками использования нормативных правовых актов в области защиты информации; – навыками разработки руководящих документов по защите информации. 	

В результате освоения дисциплины обучающийся должен

3.1 Знать:	
3.1.1	– основные термины, употребляющиеся в сфере защиты web-приложений;
3.1.2	– классы атак на web-приложения, методы защиты от них.
3.2 Уметь:	
3.2.1	– использовать изученные механизмы защиты от распространенных атак.
3.3 Владеть:	
3.3.1	– анализа исходных кодов, настроек конфигурации с целью обнаружения web-уязвимостей.

4. ОБЪЕМ ДИСЦИПЛИНЫ (МОДУЛЯ)

Общая трудоемкость	5 ЗЕТ
Часов по учебному плану : 180 в том числе : аудиторные занятия : 72 самостоятельная работа : 72 часов на контроль : 36	Виды контроля в семестрах: экзамены 10

5. СТРУКТУРА И СОДЕРЖАНИЕ ДИСЦИПЛИНЫ (МОДУЛЯ)

Код занятия	Наименование разделов и тем /вид занятия/	Семестр / Курс	Часов	Литература
	Раздел 1. Основы безопасности web-приложений			
1.1	Объекты web-сервисов. Проблемы безопасности web-клиентов. Методы взлома web-приложений. Сценарии компьютерных атак. Системы обнаружения вторжений, фаерволлы, используемые в web-технологиях. /Лек/	10	10	Л1.1 Л1.2 Л1.3 Л1.4Л2.1 Л2.2 Л2.3 Л2.4
1.2	Объекты web-сервисов. Проблемы безопасности web-клиентов. Методы взлома web-приложений. Сценарии компьютерных атак. Системы обнаружения вторжений, фаерволлы, используемые в web-технологиях. /Пр/	10	10	Л1.1 Л1.2 Л1.3 Л1.4Л2.1 Л2.2 Л2.3 Л2.4
1.3	Основы безопасности web-приложений. Проработка лекционного материала. /Ср/	10	20	Л1.1 Л1.2 Л1.3 Л1.4Л2.1 Л2.2 Л2.3 Л2.4
	Раздел 2. Атаки на web-приложения			

Рабочая программа дисциплины "Защита web-приложений" по направлению подготовки (специальности) "Компьютерная безопасность" направленности (профилю) специализация N 1 "Анализ безопасности компьютерных систем": ФГБОУ ВО «ЧелГУ»				стр. 6
2.1	Классы атак. Уязвимости аутентификации. Brute Force. Недостаточная аутентификация. Небезопасное восстановление паролей. Атаки типа «Credential/Session Prediction», «Insufficient Authorization», «Insufficient Session Expiration», «Session Fixation». Атаки на клиентов. Подмена содержимого. Межсайтовое исполнение сценариев. Расщепление HTTP-запроса. Атака на функции форматирования строк. Переполнение буфера. Внедрение операторов LDAP. Выполнение команд ОС. Внедрение операторов SQL. Слепые инъекции. Внедрение серверных сценариев SSI. Внедрение операторов XPath. Идентификация web-приложений. Information Leakage. Path Traversal. Предсказуемое расположение ресурсов. Злоупотребление функциональными возможностями. Отказ в обслуживании. Флудинг. Cross Site Request Forgery. /Лек/	10	14	Л1.1 Л1.2 Л1.3 Л1.4Л2.1 Л2.2 Л2.3 Л2.4
2.2	Классы атак. Уязвимости аутентификации. Brute Force. Недостаточная аутентификация. Небезопасное восстановление паролей. Атаки типа «Credential/Session Prediction», «Insufficient Authorization», «Insufficient Session Expiration», «Session Fixation». Атаки на клиентов. Подмена содержимого. Межсайтовое исполнение сценариев. Расщепление HTTP-запроса. Атака на функции форматирования строк. Переполнение буфера. Внедрение операторов LDAP. Выполнение команд ОС. Внедрение операторов SQL. Слепые инъекции. Внедрение серверных сценариев SSI. Внедрение операторов XPath. Идентификация web-приложений. Information Leakage. Path Traversal. Предсказуемое расположение ресурсов. Злоупотребление функциональными возможностями. Отказ в обслуживании. Флудинг. Cross Site Request Forgery. /Пр/	10	14	Л1.1 Л1.2 Л1.3 Л1.4Л2.1 Л2.2 Л2.3 Л2.4
2.3	Атаки на web-приложения. Проработка лекционного материала и материала практических занятий. /Ср/	10	24	Л1.1 Л1.2 Л1.3 Л1.4Л2.1 Л2.2 Л2.3 Л2.4
Раздел 3. Защита web-приложений				
3.1	Администрирование web-серверов. Обработка входных данных. Анализаторы исходных кодов. Web application firewall. Фильтрация sql-запросов. Параметризованные запросы. Сканеры web- приложений /Лек/	10	12	Л1.1 Л1.2 Л1.3 Л1.4Л2.1 Л2.2 Л2.3 Л2.4
3.2	Администрирование web-серверов. Обработка входных данных. Анализаторы исходных кодов. Web application firewall. Фильтрация sql-запросов. Параметризованные запросы. Сканеры web- приложений. /Пр/	10	12	Л1.1 Л1.2 Л1.3 Л1.4Л2.1 Л2.2 Л2.3 Л2.4
3.3	Администрирование web-серверов. Обработка входных данных. Анализаторы исходных кодов. Web application firewall. Фильтрация sql-запросов. Параметризованные запросы. Сканеры web- приложений. Проработка лекционного материала и материала практических занятий. /Ср/	10	28	Л1.1 Л1.2 Л1.3 Л1.4Л2.1 Л2.2 Л2.3 Л2.4

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

Список вопросов к экзамену

1. Структура web-сервиса.
2. Безопасность web-клиентов.
3. Системы обнаружения вторжений.
4. Web-фаерволлы.
5. Классы атак на web-приложения.
6. Виды атак на протоколы аутентификации.
7. Виды атак на протоколы авторизации.
8. Уязвимости по подмене содержимого.
9. Атаки на web-клиентов.

10. Межсайтовое исполнение сценариев.
11. Расщепление HTTP-запроса.
12. Понятие и защита от SQL-инъекций.
13. Основные виды SQL-инъекций.
14. Слепые SQL-инъекции, методы обнаружения и защиты.
15. Уязвимости по раскрытию информации.
16. Логические уязвимости web-приложений.
17. Атаки по исполнению кода на стороне сервера.
18. Основные правила администрирования web-серверов.
19. Методы анализа исходных кодов web-приложений.
20. Понятие и назначение WAF.
21. Правила обработки входных данных.

6.4. Критерии оценивания

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	Скембрей, Шема А. А., Чекатков	Секреты хакеров. Безопасность Web-приложений - готовые решения	М.: Вильямс, 2003	
Л1.2	Оглтри Т.	Firewalls. Практическое применение межсетевых экранов (https://e.lanbook.com/books/element.php?pl1_cid=25&pl1_id=1075)	Москва : ДМК Пресс, 2008	ЭБС
Л1.3	Форристал Д., Брумс К., Симонис Д., Бегнолл Б.	Защита от хакеров Web-приложений (https://e.lanbook.com/books/element.php?pl1_cid=25&pl1_id=1116)	Москва : ДМК Пресс, 2008	ЭБС
Л1.4	Скрыпников А. В., Арапов Д. В., Денисенко В. В., Герасимова Т. Д.	Защита Web-приложений: учебное пособие (https://biblioclub.ru/index.php?page=book&id=612405)	Воронеж : Воронежский государственный университет инженерных технологий, 2020	ЭБС

7.1.2. Дополнительная литература

	Авторы, составители	Заглавие	Издательство, год	Ресурс
Л2.1	Медведовский И. Д., Семьянов П. В., Леонов Д. Г.	Атака на Internet (http://e.lanbook.com/books/element.php?pl1_cid=25&pl1_id=1131)	Москва : ДМК Пресс, 2006	ЭБС
Л2.2	Марухленко А. Л., Марухленко Л. О., Ефремов М. А.	Разработка защищённых интерфейсов Web-приложений: учебное пособие (https://biblioclub.ru/index.php?page=book&id=599050)	Москва, Берлин : Директ-Медиа, 2021	ЭБС
Л2.3	Сычев Ю.Н.	Защита информации и информационная безопасность: учебное пособие (http://znanium.com/catalog/document?id=366835)	Москва : ООО "Научно-издательский центр ИНФРА-М", 2021	ЭБС
Л2.4	Гузовский А. Ф.	Проектирование и разработка web-приложений: учебное пособие для спо (https://urait.ru/bcode/475437)	Москва : Юрайт, 2021	ЭБС

7.3 Перечень информационных технологий

7.3.1 Программное обеспечение

Adobe Reader
 Notepad++
 VirtualBox
 Visual Studio

7.3.2 Профессиональные базы данных и информационно-справочные системы

Рабочая программа дисциплины "Защита web-приложений" по направлению подготовки (специальности) "Компьютерная безопасность" направленности (профилю) специализация N 1 "Анализ безопасности компьютерных систем": ФГБОУ ВО «ЧелГУ»	стр. 8
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 учебных лабораториях технических средств защиты информации и "Сетевой полигон" (ауд. 421, 423, учебный корпус №1). Материально-техническое обеспечение приведено в паспортах лабораторий.
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)

<p>При изучении данной дисциплины используются лекционные 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.</p> <p>Рекомендуется перед каждым лекционным занятием выполнить домашнее задание, что позволит лучше усвоить предыдущий материал, и изучить лекционный материал по предстоящей теме. Студенту желательно проявлять активное участие в 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.</p> <p>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 YouTube, форумы, электронная почта и др.).</p> <p>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.</p> <p>Доступ обучающегося к учебным ресурсам в режиме отложенного времени, самостоятельной работы осуществляется через сеть Интернет в удобном для него месте, времени и темпе.</p> <p>При обучении лиц с ограниченными возможностями здоровья электронное обучение, дистанционные образовательные технологии предусматривают возможность приема-передачи информации в доступных для них формах.</p> <p>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</p>

«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 «EIBraile-W14J G2»; ноутбуки с программной экранного доступа NVDA; электронные увеличители для удаленного просмотра; видеувеличители 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:

- 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.