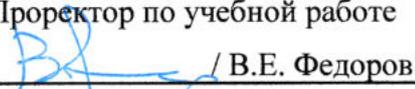


Документ подписан простой электронной подписью Информация о владельце: ФИО: Таскаев Сергей Валерьевич Должность: Ректор Дата подписания: 02.04.2021 16:09:05 Уникальный программный ключ: 04c19ed8bfb98f3b6cb77a486b9a8788b8322323	МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИИ Федеральное государственное бюджетное образовательное учреждение высшего образования «Челябинский государственный университет» (ФГБОУ ВО «ЧелГУ»)	стр. 1
--	--	--------



УТВЕРЖДАЮ  
 Проректор по учебной работе  
 / В.Е. Федоров  
 « 30 » 2021 г.

**Рабочая программа дисциплины (модуля)\***  
**Защита информации**

Направление подготовки (специальность)

02.03.02 Фундаментальная информатика и информационные технологии

Направленность (профиль)

Инженерия программного обеспечения

Присваиваемая квалификация (степень)

бакалавр

Форма обучения

очно-заочная

Год 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 Института информационных технологий

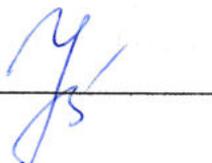
Протокол заседания № 2 «30» августа 2021 г.

Председатель Ученого совета  
ИИТ



Ю.В. Петриченко

Секретарь Ученого совета  
ИИТ



И.А. Колоскова

**Рабочая программа дисциплины (модуля) одобрена и рекомендована кафедрой**

Информационных технологий и экономической информатики

Протокол заседания № 2 «30» августа 2021 г.

И.о. заведующего кафедрой



Петриченко Ю.В.

Автор (составитель)



к.т.н., доцент Косенко М.Ю.

**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

### 1. ЦЕЛИ ОСВОЕНИЯ ДИСЦИПЛИНЫ

Целью преподавания дисциплины является ознакомление студентов с современными системами информационной безопасности, организационными и техническими мерами защиты информации, экономическими и правовыми принципами их функционирования, а также возможностями использования методов защиты информации в работе с информационными ресурсами в различных областях экономики и бизнеса.

Задачами изучения дисциплины являются:

1. познакомить студентов с определением, классификацией и характеристиками информационной безопасности;
2. познакомить с организационными и экономическими аспектами работы с информационными ресурсами и методами оценки эффективности их безопасности;
3. дать представление об особенностях информационной безопасности, сегментах и участниках информационного рынка, особенностях формирования безопасности информации;
4. рассмотреть основные технологические принципы безопасности мировых информационных ресурсов на основе глобальной сети Internet;
5. рассмотреть основные механизмы обеспечения безопасности ресурсов Internet.

Результаты обучения по дисциплине направлены на достижение индикаторов:

- УК-4.1 Имеет представление о правилах и принципах деловой устной и письменной коммуникации на государственном языке Российской Федерации и иностранном(ых) языке(ах)
- УК-4.2 Демонстрирует умение осуществлять деловую коммуникацию в устной и письменной формах, использовать методы и навыки делового общения
- УК-4.3 Имеет навыки делового общения на государственном языке Российской Федерации и иностранном(ых) языке(ах)
- ПК-1.1. Демонстрирует знание основ операционных систем, сетевых технологий, языков программирования, баз данных и технологий обработки данных, библиотек и пакетов программ, языков и методов формальных спецификаций
- ПК-1.2. Демонстрирует умения разрабатывать системное и прикладное программное обеспечение с использованием языков и технологий программирования, баз данных, сетевых технологий и операционных систем
- ПК-1.3. Имеет практический опыт использования операционных систем, современных языков программирования, библиотек и пакетов программ, систем управления базами данных и технологий обработки данных

### 2. МЕСТО ДИСЦИПЛИНЫ В СТРУКТУРЕ ОПОП

Цикл (раздел) ОПОП:

К.М.03.05

#### 2.1 Требования к предварительной подготовке обучающегося:

Основа дисциплины состоит из базовых знаний полученных из следующих дисциплин: «Программирование»; «Операционные системы»; «Базы и хранилища данных»; «Сети и телекоммуникации».

Программирование

Операционные системы

Базы и хранилища данных

Компьютерные сети

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

Знания, полученные в данной дисциплине, могут быть использованы для написания выпускной квалификационной работы.

Защита выпускной квалификационной работы, включая подготовку к процедуре защиты и процедуру защиты

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

**УК-4: Способен осуществлять деловую коммуникацию в устной и письменной формах на государственном языке Российской Федерации и иностранном(ых) языке(ах)**

#### Знать:

понятие информационных угроз и их виды, подходы к оценке информационных рисков; основные принципы функционирования сетей и методы обеспечения их безопасности; требования к подготовке презентаций, оформлению научно-технических отчетов.

#### Уметь:

применять методы оценки рисков информационной безопасности, применять компьютер для производства работ в области защиты информации; настраивать основные средства обеспечения сетевой безопасности; представлять результаты работы в виде статей и докладов.

#### Владеть:

Навыками описания выявленных уязвимостей и рекомендаций по их устранению

**ПК-1: Способность применять в профессиональной деятельности современные языки программирования и технологии обработки данных, операционные системы, электронные библиотеки и пакеты программ, сетевые технологии, системы управления базами данных.**

#### Знать:

этапы построения системы защиты информации, понятие политики безопасности.

#### Уметь:

применять основные методы и средства обеспечения безопасности.

**Владеть:**

навыками настройки безопасности в Windows системе.

**4. ОБЪЕМ ДИСЦИПЛИНЫ (МОДУЛЯ)**

<b>Общая трудоемкость</b>	<b>6 ЗЕТ</b>
Часов по учебному плану : 216 в том числе : аудиторные занятия : 8 самостоятельная работа : 172 часов на контроль : 36	Виды контроля в семестрах:  экзамены 7

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

Код занятия	Наименование разделов и тем /вид занятия/	Семестр / Курс	Часов	Литература
<b>Раздел 1. Основы безопасности информационных технологий</b>				
1.1	Изучение специальной терминологии, используемой в курсе «Информационная безопасность». Создание личного терминологического словаря. /Пр/	7	1	Л1.1 Л1.2 Л1.3 Л2.1 Л2.2 Л2.3 Л2.4 Л2.5 Л2.6 Л2.7 Э1 Э2 Э3
1.2	Требования к системам и средствам защиты информации от несанкционированного доступа. /Ср/	7	7	Л1.1 Л1.2 Л1.3 Л2.1 Л2.2 Л2.3 Л2.4 Л2.5 Л2.6 Л2.7 Э1 Э2 Э3
<b>Раздел 2. Обеспечение безопасности информационных технологий</b>				
2.1	Организационная структура системы обеспечения информационной безопасности. Обязанности конечных пользователей и ответственных за ОИБ в подразделениях. Инструкции по организации парольной и антивирусной защиты. Определение требований к защите ресурсов. Основные задачи подразделения обеспечения информационной безопасности. Концепция информационной безопасности организации /Лек/	7	1	Л1.1 Л1.2 Л1.3 Л2.1 Л2.2 Л2.3 Л2.4 Л2.5 Л2.6 Л2.7 Э1 Э2 Э3
2.2	Анализ способов хранения паролей на сайтах. Изучение методов хранения паролей. Поиск потенциально небезопасных сайтов. Безопасность информации в корпоративных информационных системах. Внутренние угрозы. Законодательство в сфере информационной безопасности. Анализ прецедентов /Пр/	7	1	Л1.1 Л1.2 Л1.3 Л2.1 Л2.2 Л2.3 Л2.4 Л2.5 Л2.6 Л2.7 Э1 Э2 Э3
2.3	Разработка модели разграничения доступа к информации. Управление доступом в компьютерных системах. Задачи контроля и обеспечения безопасности информации. Разрушающие программные воздействия и защита от них. Обеспечение целостности информации /Ср/	7	35	Л1.1 Л1.2 Л1.3 Л2.1 Л2.2 Л2.3 Л2.4 Л2.5 Л2.6 Л2.7 Э1 Э2 Э3
<b>Раздел 3. Средства защиты информации от несанкционированного доступа</b>				
3.1	Системы авторизации операционных систем. Изучить работу шифрованной файловой системы EFS: особенности шифрования, файлов и папок, предназначение и работа агента восстановления, способы хранения ключевой информации. /Пр/	7	1	Л1.1 Л1.2 Л1.3 Л2.1 Л2.2 Л2.3 Л2.4 Л2.5 Л2.6 Л2.7 Э1 Э2 Э3
3.2	Программно-аппаратные средства шифрования. Методы распределения и хранения ключевой и парольной информации /Ср/	7	16	Л1.1 Л1.2 Л1.3 Л2.1 Л2.2 Л2.3 Л2.4 Л2.5 Л2.6 Л2.7 Э1 Э2 Э3
<b>Раздел 4. Обеспечение безопасности компьютерных систем и сетей</b>				
4.1	Угрозы, уязвимости и атаки в сетях. Сетевые средства защиты. /Лек/	7	1	Л1.1 Л1.2 Л1.3 Л2.1 Л2.2 Л2.3 Л2.4 Л2.5 Л2.6 Л2.7 Э1 Э2 Э3
4.2	Обеспечение безопасности межсетевое взаимодействие. Удаленные сетевые атаки. Технологии межсетевых экранов. Системы обнаружения атак и вторжений. Виртуальные частные сети /Ср/	7	35	Л1.1 Л1.2 Л1.3 Л2.1 Л2.2 Л2.3 Л2.4 Л2.5 Л2.6 Л2.7 Э1 Э2 Э3
<b>Раздел 5. Обеспечение безопасности веб-ресурсов.</b>				
5.1	Обнаружение, эксплуатация и предотвращение веб-уязвимостей (SQL Injection: Types of SQL Injection, Different, DBMSs, Blind SQL Injection, Cross-Site Scripting (XSS) Attacks, Cross-Site Request Forgery (CSRF) Attack, Command Injection Attacks, File Injection Attacks, Session Injection Attacks, Weak authentication and session management, Security Misconfiguration, Insufficient Transport Layer Protection). /Пр/	7	3	Л1.1 Л1.2 Л1.3 Л2.1 Л2.2 Л2.3 Л2.4 Л2.5 Л2.6 Л2.7 Э1 Э2 Э3
5.2	Обеспечение безопасности веб-ресурсов. /Ср/	7	79	Л1.1 Л1.2 Л1.3 Л2.1 Л2.2

Рабочая программа дисциплины "Защита информации" по направлению подготовки (специальности) "Фундаментальная информатика и информационные технологии" направленности (профилю) Инженерия программного обеспечения ФГБОУ ВО «ЧелГУ»				стр. 6
				Л2.3 Л2.4 Л2.5 Л2.6 Л2.7 Э1 Э2 Э3
	<b>Раздел 6. Экзамен</b>			
6.1	Экзамен /Экзамен/	7	36	Л1.1 Л1.2 Л1.3 Л2.1 Л2.2 Л2.3 Л2.4 Л2.5 Л2.6 Л2.7 Э1 Э2 Э3

<b>6. ФОНД ОЦЕНОЧНЫХ СРЕДСТВ</b>	
<b>6.1. Перечень видов оценочных средств</b>	
Проверка практической работы Тестирование	
<b>6.2. Типовые контрольные задания и иные материалы для текущей аттестации</b>	
Пример тестового задания:	
<p>1. Какое свойство компонента (ресурса) АС заключается в том, что он доступен только тем субъектам (пользователям, программам, процессам), которым предоставлены на то соответствующие полномочия?</p> <p>a конфиденциальность b целостность c доступность d неотказуемость e подотчётность f достоверность g аутентичность</p> <p>2. Какое свойство компонента (ресурса) АС предполагает, что он может быть модифицирован только субъектом, имеющим для этого соответствующие права?</p> <p>a целостность b конфиденциальность c доступность d неотказуемость e подотчётность f достоверность g аутентичность</p> <p>3. Какое свойство компонента (ресурса) АС означает, что имеющий соответствующие полномочия субъект может без особых проблем получить своевременный доступ к необходимому компоненту системы?</p> <p>a доступность b конфиденциальность c целостность d неотказуемость e подотчётность f достоверность g аутентичность</p> <p>В ходе обучения дисциплине обучающийся должен выполнить набор лабораторных/практических работ.</p> <ol style="list-style-type: none"> <li>Изучение специальной терминологии, используемой в курсе «Информационная безопасность». Создание личного терминологического словаря.</li> <li>Анализ способов хранения паролей на сайтах. Изучение методов хранения паролей. Поиск потенциально небезопасных сайтов.</li> <li>Безопасность информации в корпоративных информационных системах. Внутренние угрозы.</li> <li>Законодательство в сфере информационной безопасности. Анализ прецедентов.</li> <li>Системы авторизации операционных систем.</li> <li>Изучить работу шифрованной файловой системы EFS: особенности шифрования, файлов и папок, предназначение и работа агента восстановления, способы хранения ключевой информации.</li> <li>Обнаружение и эксплуатация уязвимости SQL Injection: Types of SQL Injection, Different DBMSs, Blind SQL Injection</li> <li>Обнаружение и эксплуатация уязвимости Cross-Site Scripting (XSS) Attacks</li> <li>Обнаружение и эксплуатация уязвимости Cross-Site Request Forgery (CSRF) Attack</li> <li>Обнаружение и эксплуатация уязвимости Command Injection Attacks</li> <li>Обнаружение и эксплуатация уязвимости File Injection Attacks</li> <li>Обнаружение и эксплуатация уязвимости Session Injection Attacks</li> <li>Обнаружение и эксплуатация уязвимости Weak authentication and session management</li> <li>Обнаружение и эксплуатация уязвимости Security Misconfiguration</li> <li>Обнаружение и эксплуатация уязвимости Insufficient Transport Layer Protection</li> </ol>	

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

Примерные вопросы тестового задания:

Что из перечисленного не должно отражаться в политике информационной безопасности предприятия?

- a. цели защиты информации
- b. какие ресурсы подлежат защите
- c. от каких угроз защищаются ресурсы
- d. кто несёт ответственность за защищённость ресурсов
- e. стоимость защищаемых ресурсов
- f. сфера действия политики
- g. порядок информирования об инцидентах
- h. какие документы дополняют политику безопасности
- i. организация взаимодействия защищаемых ресурсов
- j. Ничего из представленного

Комплекс аппаратных или программных средств, осуществляющий контроль и фильтрацию проходящих через него сетевых пакетов в соответствии с заданными правилами, это?

- a. межсетевой экран
- b. система обнаружения атак
- c. антивирусное средство
- d. средства контроля доступа и аутентификации

Какие межсетевые экраны проверяют факт, что пакет является либо запросом на TCP-соединение, либо представляет данные, относящиеся к уже установленному соединению, либо относится к виртуальному соединению между двумя транспортными уровнями?

- a. межсетевые экраны уровня соединения
- b. межсетевые экраны прикладного уровня
- c. межсетевые экраны с динамической фильтрацией пакетов
- d. межсетевые экраны инспекции состояний
- e. межсетевые экраны уровня ядра

### 6.4. Критерии оценивания

При собеседовании выделяются критерии, по которым оцениваются знания учащихся.

Отметка «отлично» ставится в том случае, если по двум из трех критериев ответ оценивается «отлично» и по одному – на «хорошо».

Отметка «хорошо» – если по двум критериям – не ниже «хорошо» и по одному «удовлетворительно».

Отметка «удовлетворительно» – если по двум критериям не ниже «удовлетворительно» и по одному – «неудовлетворительно».

Отметка «неудовлетворительно» – если по двум и более критериям «неудовлетворительно».

Критерии:

Владение понятийным аппаратом

Владение фактическим материалом по теме

Логичность изложения материала.

Каждую практическую работу можно зачесть, если:

1 - Обучающийся: свободно ориентируется в терминологии; способен привести примеры; свободно может ответить на дополнительные вопросы.

2-15 - Обучающийся: свободно ориентируется в материале тематики; владеет навыками настройки безопасности; может анализировать информацию и принимать решения; свободно может ответить на дополнительные вопросы.

Оценка теста:

Набранная сумма баллов - оценка

Менее 60 - неудовлетворительно;

60-75 - удовлетворительно;

76-90 - хорошо;

91-100 - отлично.

Итоговая оценка за дисциплину формируется следующим образом:

Каждая практическая работа оценивается в 4 балла итоговой оценки. Итоговый тест дает 40 баллов итоговой оценки. Максимум можно набрать 100 баллов за дисциплину.

Итоговая оценка конвертируется в 5 бальную систему:

Набранная сумма баллов - оценка

Менее 60 – неудовлетворительно;

60-75 – удовлетворительно (зачет);

76-89 – хорошо (зачет);

90-100 – отлично (зачет).

Требования (критериальные показатели) к уровням освоения программы дисциплины во втором семестре изучения дисциплины

«Отлично» (5) – студент глубоко и полно владеет содержанием учебного материала; умеет связывать теорию с практикой, решает микроэкономические задачи, теоретические выводы подтверждает примерами, фактами, данными научных исследований; осуществляет межпредметные связи, предложения. Делает выводы логично, четко. Ясно и кратко излагает ответы на поставленные вопросы; умеет обосновывать свои суждения и профессионально- личностную позицию по излагаемому вопросу. Ответ носит самостоятельный характер.

«Хорошо» (4) – ответ студента соответствует указанным выше критерия, но содержание ответа имеет отдельные неточности (несущественные ошибки) в изложении теоретического и практического материала, отличается меньшей обстоятельностью, глубиной, обоснованностью и полнотой; допущенные ошибки исправляются студентом после дополнительных вопросов экзаменатора.

«Удовлетворительно» (3) – студент обнаруживает знание и понимание основных положений учебного материала, но излагает его неполно, непоследовательно, допускает неточности и существенные ошибки в определении понятий, формулировке положений, не привлекает для аргументации ответа основные положения исследовательских, концептуальных и нормативных документов, не умеет обосновать свои суждения; наблюдается нарушение логики изложения. Ответ отличается низким уровнем самостоятельности, не содержит собственной профессионально- личностной позиции.

«Неудовлетворительно» (2) – студент имеет разрозненные, бессистемные знания: не умеет выделять главное и второстепенное; допускает ошибки в определении понятий, формулировке теоретических положений, искажает их смысл; не ориентируется в нормативно-концептуальных, программно-методических, исследовательских материалах, беспорядочно и неуверенно излагает материал; не умеет соединять теоретические положения с практикой; не умеет применять знания для обоснования и объяснения фактов, не устанавливает межпредметные связи.

## 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	Жук А.П., Жук Е.П.	Защита информации ( <a href="http://znanium.com/catalog/document?id=367588">http://znanium.com/catalog/document?id=367588</a> ) Дата обращения: 2021-01-20	Москва : Издательский Центр РИОР, 2021	ЭБС
Л1.2	Хорев П. Б.	Программно-аппаратная защита информации ( <a href="http://znanium.com/catalog/document?id=365036">http://znanium.com/catalog/document?id=365036</a> ) Дата обращения: 2021-01-20	Москва : ООО "Научно-издательский центр ИНФРА-М", 2021	ЭБС
Л1.3	Баранова Е.К., Бабаш А.В.	Информационная безопасность и защита информации ( <a href="http://znanium.com/catalog/document?id=364911">http://znanium.com/catalog/document?id=364911</a> ) Дата обращения: 2021-01-20	Москва : Издательский Центр РИОР, 2021	ЭБС

#### 7.1.2. Дополнительная литература

	Авторы, составители	Заглавие	Издательство, год	Ресурс
Л2.1	Внуков А. А.	Основы информационной безопасности: защита информации ( <a href="https://urait.ru/bcode/467356">https://urait.ru/bcode/467356</a> ) Дата обращения: 2021-01-20	Москва : Юрайт, 2020	ЭБС
Л2.2	Бабенко Л. К., Ищукова Е. А.	Криптографическая защита информации: симметричное шифрование ( <a href="https://urait.ru/bcode/452871">https://urait.ru/bcode/452871</a> ) Дата обращения: 2021-01-20	Москва : Юрайт, 2020	ЭБС
Л2.3	Крамаров С.О., Тищенко Е.Н.	Криптографическая защита информации ( <a href="http://znanium.com/go.php?id=901659">http://znanium.com/go.php?id=901659</a> ) Дата обращения: 2021-01-20	Москва : Издательский Центр РИОР, 2018	ЭБС
Л2.4	Шаньгин В.Ф.	Комплексная защита информации в корпоративных системах ( <a href="http://znanium.com/go.php?id=937502">http://znanium.com/go.php?id=937502</a> ) Дата обращения: 2021-01-20	Москва : Издательский Дом "ФОРУМ", 2018	ЭБС
Л2.5	Панфилова О.А., Крюкова Д.Ю.	Информационная безопасность и защита информации ( <a href="http://znanium.com/catalog/document?id=370184">http://znanium.com/catalog/document?id=370184</a> ) Дата обращения: 2021-01-20	Вологда : федеральное казенное образовательное учреждение высшего образования «Вологодский институт права и экономики Федеральной службы исполнения	ЭБС

Рабочая программа дисциплины "Защита информации" по направлению подготовки (специальности) "Фундаментальная информатика и информационные технологии" направленности (профилю) Инженерия программного обеспечения ФГБОУ ВО «ЧелГУ»	стр. 9
---	--------

Л2.6	Смирнов В. И.	Защита информации: лабораторный практикум ( <a href="http://biblioclub.ru/index.php?page=book&amp;id=476512">http://biblioclub.ru/index.php?page=book&amp;id=476512</a> ) Дата обращения: 2021-01-20	наказаний», 2018 Йошкар-Ола : Поволжский государственный технологический университет, 2017	ЭБС
Л2.7	Баранова Е.К., Бабаш А.В.	Информационная безопасность и защита информации ( <a href="http://znanium.com/go.php?id=763644">http://znanium.com/go.php?id=763644</a> ) Дата обращения: 2021-01-20	Москва : Издательский Центр РИОР, 2017	ЭБС

## 7.2. Перечень ресурсов информационно-телекоммуникационной сети "Интернет"

Э1	Лань [Электронный ресурс] : электронно-библиотечная система (ЭБС) / издательство Лань. – URL: <a href="http://e.lanbook.com">http://e.lanbook.com</a>
Э2	Университетская библиотека онлайн [Электронный ресурс] : электронно-библиотечная система (ЭБС) / ООО Директмедиа Паблишинг. – URL: <a href="http://biblioclub.ru">http://biblioclub.ru</a>
Э3	Юрайт [Электронный ресурс] : электронно-библиотечная система (ЭБС) / издательство Юрайт. – URL: <a href="https://biblio-online.ru">https://biblio-online.ru</a>

## 7.3 Перечень информационных технологий

### 7.3.1 Программное обеспечение

LMS Moodle
MS Office365
Python3
Wireshark

### 7.3.2. Профессиональные базы данных и информационно-справочные системы

1. Научная электронная библиотека eLIBRARY.RU (<https://elibrary.ru/defaultx.asp?>) eLIBRARY.RU : научная электронная библиотека : сайт. – Москва, 2000 – . – URL: <https://elibrary.ru>. – Режим доступа: для зарегистрир. пользователей. – Текст : электронный.
2. Национальная электронная библиотека (НЭБ) (<https://rusneb.ru/>) Национальная электронная библиотека (НЭБ) : объединенный электронный каталог фондов российских библиотек : сайт. – URL: <http://нэб.рф>. – Режим доступа: из читальных залов библиотеки ЧелГУ. – Текст : электронный.
3. Президентская библиотека (<https://www.prlib.ru/>) Президентская библиотека : электронная национальная библиотека : сайт / ФГБУ Президентская библиотека имени Б. Н. Ельцина. – СанктПетербург, 2009 – . – URL: <https://www.prlib.ru/>. – Текст : электронный.
4. Справочно-правовая система «КонсультантПлюс» (<http://www.consultant.ru/>) КонсультантПлюс : справочно- правовая система : база данных / Региональный центр правовой информации Информправо. – Москва, 1992 – . – Режим доступа: из читальных залов библиотеки. – Текст : электронный.

## 8. МАТЕРИАЛЬНО-ТЕХНИЧЕСКОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ

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: доска, парты, мультимедийное и аудиооборудование.

Для проведения занятий лекционного типа предлагаются наборы демонстрационного оборудования и учебно- наглядных пособий: цифровые образовательные ресурсы, а также используется переносное и / или стационарное мультимедийное оборудование (экран, ноутбук, проектор, колонки).

Для семинарских занятий используются аудитории оснащенные обычной доской, партами, переносным мультимедийным и аудиооборудованием (в случае необходимости).

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

В качестве учебных аудиторий для проведения занятий лекционного типа, занятий семинарского типа, групповых и индивидуальных консультаций, текущего контроля и промежуточной аттестации при применении дистанционных образовательных технологий используются помещения для проведения вебинаров – учебные аудитории. В них имеются мультимедийный проектор Epson EB-925, ноутбуки DEXP W670SFQ, Core i7, 8 гб, микрофон, веб-камера, всепогодная акустическая система Magnat Symbol Pro 160 black, маркерная доска, стол студента (сборный), стол преподавателя, стулья.

## 9. МЕТОДИЧЕСКИЕ УКАЗАНИЯ ДЛЯ ОБУЧАЮЩИХСЯ ПО ОСВОЕНИЮ ДИСЦИПЛИНЫ

Успешное изучение курса требует от обучающихся посещения лекций, активной работы на семинарах, выполнения всех учебных заданий преподавателя, ознакомления с базовыми учебниками, основной и дополнительной литературой. Запись лекции – одна из форм активной работы студентов, требующая навыков и умения кратко, схематично, последовательно и логично фиксировать основные положения, выводы, обобщения, формулировки. Последующая работа над текстом лекции воскрешает в памяти ее содержание, позволяет развивать экономическое мышление. В конце лекции преподаватель оставляет время (5 минут) для того, чтобы студенты имели возможность задать уточняющие вопросы по изучаемому материалу.

Важным методом обучения является самостоятельная работа студентов с учебно-методическими материалами, научной литературой. При изучении дисциплины необходимо изучить вопросы, которые преподаватель вынес на самостоятельное изучение,

быть готовым к обсуждению этих вопросов.

К промежуточной аттестации необходимо готовиться целенаправленно, регулярно, систематически и с первых дней обучения по данной дисциплине. После этого у обучающегося должно сформироваться четкое представление об объеме и характере знаний и умений, которыми надо будет овладеть по дисциплине. Систематическое выполнение учебной работы на лекциях и семинарских занятиях позволит успешно освоить дисциплину.

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, 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 «ElBraille-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-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 Clever 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.