Рабочая программа дисциплины (модуля)*

Защита информации

Направление подготовки (специальность)

09.03.04 Программная инженерия

Направленность (профиль)

Разработка программно-информационных систем

Присваиваемая квалификация (степень)

бакалавр

Форма обучения

очная

Год(ы) набора

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

Челябинск 2024 г.

09.03.04 Программная инженерия, Разработка программно-информационных систем, бакалавр, *Защита информации*, 2025, очная

Проректор по учебной работе утверждено 24.02.2025 А.А. Саламатов

Ученым советом института информационных технологий

Протокол заседания № 6 от 20.02.2025

Председатель Ученого совета
института информационных
технологий согласовано Ю. В. Петриченко

Заседанием кафедры информационных технологий и экономической информатики

Протокол заседания № 6 от 20.02.2025

И. о. заведующего кафедрой согласовано С.А. Скрипов

Автор (составитель) А.В. Митянина

Структура рабочей программы соответствует приказу ректора ФГБОУ ВО «ЧелГУ» от «13» апреля 2021 г. № 247-1

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, основ проектирования интерфейсов, языков и методов формальных спецификаций

ПК-1.2. Демонстрирует умения разрабатывать системное и прикладное программного обеспечение с использованием языков и технологий программирования, баз данных, сетевых технологий и операционных систем, языков и методов формальных спецификаций

ПК-1.3. Имеет практический опыт использования операционных систем, современных языков программирования, систем управления базами данных и технологий обработки данных, средств разработки программного интерфейса

2. МЕСТО ДИСЦИПЛИНЫ В СТРУКТУРЕ ОПОП

Цикл (раздел) ОПОП:	К.М.03.06

2.1 Требования к предварительной подготовке обучающегося:

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

Операционные системы

Базы и хранилища данных

Вычислительные системы, сети и телекоммуникации

Программирование

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.

Выполнение и защита выпускной квалификационной работы

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: Владение навыками использования операционных систем, сетевых технологий, современных языков программирования, технологий обработки данных, средств разработки программного интерфейса, применения языков и методов формальных спецификаций, систем 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.

В результате освоения дисциплины обучающийся должен

3.1	**Знать:**
3.1.1	понятие информационных угроз и их виды, методы обеспечения безопасности
3.2	**Уметь:**
3.2.1	применять основные методы и средства обеспечения безопасности
3.3	**Владеть:**
3.3.1	навыками использования средств обеспечения информационной безопасности

4. ОБЪЕМ ДИСЦИПЛИНЫ (МОДУЛЯ)

Общая трудоемкость	**6 ЗЕТ**
Часов по учебному плану : 216 в том числе : аудиторные занятия : 48 самостоятельная работа : 141 часов на контроль : 18 контактная работа: 57 ИКР: 9	Виды контроля в семестрах: экзамены 7

5. СТРУКТУРА И СОДЕРЖАНИЕ ДИСЦИПЛИНЫ (МОДУЛЯ)

Код занятия	Наименование разделов и тем /вид занятия/	Семестр / Курс	Часов	Литература
	Раздел 1. Иная контактная работа			
1.1	Индивидуальные консультации, текущий контроль /ИКР/	7	9	Л1.1 Л1.2Л2.1 Л2.2 Л2.3 Э4 Э5 Э6
	Раздел 2. Раздел 1. Основы безопасности информационных технологий			

2.1	Актуальность проблемы обеспечение безопасности информационных технологий. Основные понятия информационной безопасности. Угрозы информационной безопасности в АС. Виды мер и основные принципы обеспечения информационной безопасности. Правовые основы обеспечения информационной безопасности. Основные защитные механизмы, используемые в СЗИ /Лек/	7	4	Л1.1 Л1.2Л2.1 Л2.2 Л2.3 Э4 Э5 Э6
2.2	Изучение специальной терминологии, используемой в курсе «Информационная безопасность». Создание личного терминологического словаря. /Пр/	7	4	Л1.1 Л1.2Л2.1 Л2.2 Л2.3 Э4 Э5 Э6
2.3	Требования к системам и средствам защиты информации от несанкционированного доступа. /Ср/	7	32	Л1.1 Л1.2Л2.1 Л2.2 Л2.3 Э4 Э5 Э6
	Раздел 3. Раздел 2. Обеспечение безопасности информационных технологий			
3.1	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	2	Л1.1 Л1.2Л2.1 Л2.2 Л2.3 Э4 Э5 Э6
3.2	Анализ способов хранения паролей на сайтах. Изучение методов хранения паролей. Поиск потенциально небезопасных сайтов /Пр/	7	2	Л1.1 Л1.2Л2.1 Л2.2 Л2.3 Э4 Э5 Э6
3.3	Безопасность информации в корпоративных информационных системах. Внутренние угрозы. /Пр/	7	2	Л1.1 Л1.2Л2.1 Л2.2 Л2.3 Э4 Э5 Э6
3.4	Законодательство в сфере информационной безопасности. Анализ прецедентов. /Пр/	7	2	Л1.1 Л1.2Л2.1 Л2.2 Л2.3 Э4 Э5 Э6
3.5	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	29	Л1.1 Л1.2Л2.1 Л2.2 Л2.3 Э4 Э5 Э6
	Раздел 4. Раздел 3. Средства защиты информации от несанкционированного доступа			
4.1	Назначение и возможности СЗИ НСД. Рекомендации по выбору средств защиты от НСД. Аппаратные средства СЗИ НСД. /Лек/	7	3	Л1.1 Л1.2Л2.1 Л2.2 Л2.3 Э4 Э5 Э6
4.2	Системы авторизации операционных систем. /Пр/	7	2	Л1.1 Л1.2Л2.1 Л2.2 Л2.3 Э4 Э5 Э6
4.3	Изучить работу шифрованной файловой системы EFS: особенности шифрования, файлов и папок, предназначение и работа агента восстановления, способы хранения ключевой информации. /Пр/	7	2	Л1.1 Л1.2Л2.1 Л2.2 Л2.3 Э4 Э5 Э6
4.4	Программно-аппаратные средства шифрования. Методы распределения и хранения ключевой и парольной информации /Ср/	7	26	Л1.1 Л1.2Л2.1 Л2.2 Л2.3 Э4 Э5 Э6
	Раздел 5. Раздел 4. Обеспечение безопасности компьютерных систем и сетей			
5.1	Угрозы, уязвимости и атаки в сетях. Сетевые средства защиты. /Лек/	7	3	Л1.1 Л1.2Л2.1 Л2.2 Л2.3 Э4 Э5 Э6

5.2	Обеспечение безопасности межсетевого взаимодействия. Удаленные сетевые атаки. Технологии межсетевых экранов. Системы обнаружения атак и вторжений. Виртуальные частные сети /Пр/	7	6	Л1.1 Л1.2Л2.1 Л2.2 Л2.3 Э4 Э5 Э6
	Раздел 6. Обеспечение безопасности веб-ресурсов.			
6.1	Уязвимости веб-ресурсов. /Лек/	7	4	Л1.1 Л1.2Л2.1 Л2.2 Л2.3 Э4 Э5 Э6
6.2	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	12	Л1.1 Л1.2Л2.1 Л2.2 Л2.3 Э4 Э5 Э6
6.3	Обеспечение безопасности веб-ресурсов /Ср/	7	54	Л1.1 Л1.2Л2.1 Л2.2 Л2.3 Э3 Э4 Э5 Э6

6. ФОНД ОЦЕНОЧНЫХ СРЕДСТВ

6.1. Перечень видов оценочных средств

Проверка практической работы
Тестирование

6.2. Типовые контрольные задания и иные материалы для текущей аттестации

Пример тестового задания:
1. Какое свойство компонента (ресурса) АС заключается в том, что он доступен только тем субъектам (пользователям, программам, процессам), которым предоставлены на то соответствующие полномочия?
a конфиденциальность
b целостность
c доступность
d неотказуемость
e подотчётность
f достоверность
g аутентичность
2. Какое свойство компонента (ресурса) АС предполагает, что он может быть модифицирован только субъектом, имеющим для этого соответствующие права?
a целостность
b конфиденциальность
c доступность
d неотказуемость
e подотчётность
f достоверность
g аутентичность
3. Какое свойство компонента (ресурса) АС означает, что имеющий соответствующие полномочия субъект может без особых проблем получить своевременный доступ к необходимому компоненту системы?
a доступность
b конфиденциальность
c целостность
d неотказуемость
e подотчётность
f достоверность
g аутентичность

В ходе обучения дисциплине обучающийся должен выполнить набор лабораторных/практических работ.
1. Изучение специальной терминологии, используемой в курсе «Информационная безопасность». Создание личного терминологического словаря.
2. Анализ способов хранения паролей на сайтах. Изучение методов хранения паролей. Поиск потенциально небезопасных сайтов.
3. Безопасность информации в корпоративных информационных системах. Внутренние угрозы.

4. Законодательство в сфере информационной безопасности. Анализ прецедентов.
5. Системы авторизации операционных систем.
6. Изучить работу шифрованной файловой системы EFS: особенности шифрования, файлов и папок, предназначение и работа агента восстановления, способы хранения ключевой информации.
7. Обнаружение и эксплуатация уязвимости SQL Injection: Types of SQL Injection, Different DBMSs, Blind SQL Injection
8. Обнаружение и эксплуатация уязвимости Cross-Site Scripting (XSS) Attacks
9. Обнаружение и эксплуатация уязвимости Cross-Site Request Forgery (CSRF) Attack
10. Обнаружение и эксплуатация уязвимости Command Injection Attacks
11. Обнаружение и эксплуатация уязвимости File Injection Attacks
12. Обнаружение и эксплуатация уязвимости Session Injection Attacks
13. Обнаружение и эксплуатация уязвимости Weak authentication and session management
14. Обнаружение и эксплуатация уязвимости Security Misconfiguration
15. Обнаружение и эксплуатация уязвимости Insufficient Transport Layer Protection

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 7 семестр формируется следующим образом:
Каждая практическая работа с 1 по 6 оценивается в 8 балла итоговой оценки. Итоговый тест дает 52 балла итоговой оценки. Максимум можно набрать 100 баллов за семестр.

Итоговая оценка за 8 семестр формируется следующим образом:
Каждая практическая работа с 7 по 15оценивается в 6 балла итоговой оценки. Итоговый тест дает 46 баллов итоговой оценки. Максимум можно набрать 100 баллов за семестр.

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	Шаньгин В.Ф.	Комплексная защита информации в корпоративных системах: учебное пособие (https://znanium.com/catalog/document?id=389857)	Москва : Издательский Дом "ФОРУМ", 2022	ЭБС
Л1.2	Хорев П. Б.	Программно-аппаратная защита информации: учебное пособие (https://znanium.com/catalog/document?id=397282)	Москва : ООО "Научно-издательский центр ИНФРА-М", 2022	ЭБС

7.1.2. Дополнительная литература

	Авторы, составители	Заглавие	Издательство, год	Ресурс
Л2.1	Голиков А. М.	Кодирование и шифрование информации в системах связи. Часть 2. Шифрование: учебное пособие для специалитета: 210601.65радиоэлектронные системы и комплексы. курс лекций, компьютерный практикум, задание на самостоятельную работу (https://e.lanbook.com/book/110225)	Москва : ТУСУР, 2016	ЭБС
Л2.2	Голиков А. М.	Кодирование и шифрование информации в системах связи. Часть 1. Кодирование.: учебное пособие для специалитетета: 210601.65 радиоэлектронные системы и комплексы. курс лекций, компьютерый практикум, задание на самостоятельную работу. (https://e.lanbook.com/book/110240)	Москва : ТУСУР, 2016	ЭБС
Л2.3	Берджесс Э.	Искусственный интеллект - для вашего бизнеса: руководство по оценке и применению (https://znanium.com/catalog/document?id=387328)	Москва : Интеллектуальная Литература, 2021	ЭБС

7.2. Перечень ресурсов информационно-телекоммуникационной сети "Интернет"

Э1	Научная электронная библиотека eLIBRARY.RU» - раздел "Журналы открытого доступа" (https://elibrary.ru/projects/subscription/rus_titles_free.asp)
Э2	Единое окно доступа к образовательным ресурсам - федеральная информационная система открытого доступа к интегральному каталогу образовательных интернет-ресурсов и к электронной библиотеке учебно- методических материалов для всех уровней образования: дошкольное, общее, среднее профессиональное, высшее, дополнительное.http://window.edu.ru
Э3	Лекториум - просветительский проект: массовые открытые онлайн-курсы, открытый видеоархив лекций вузов России https://www.lektorium.tv
Э4	Лань [Электронный ресурс] : электронно-библиотечная система (ЭБС) / издательство Лань http://e.lanbook.com
Э5	Юрайт [Электронный ресурс] : электронно-библиотечная система (ЭБС) / издательство Юрайт. https://urait.ru/
Э6	Znanium.com [Электронный ресурс] : электронно-библиотечная система (ЭБС) / Науч. электрон. б-ка http://znanium.com/

7.3 Перечень информационных технологий

7.3.1 Программное обеспечение

LMS Moodle

ПО Kaspersky

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 Президéнтская библиотéка и́мени Б. Н. Е́льцина. – 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 (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: 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.

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

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.
Основным 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. Дискуссия – коллективная форма устного представления информации. Обычно дискуссию готовит один или несколько человек, представляющих основные вопросы темы и точки зрения. Остальные участники дискуссии высказывают свои мнения и суждения. Дискуссию организует ведущий (чаще преподаватель) в обязанность которого входит предоставление слова разным участникам, сдерживание эмоциональных реакций участников и подведение итогов обсуждения.
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 информационных технологий, предоставляемых Ресурсным учебно-методическим центром по обучению инвалидов и лиц с ограниченными возможностями здоровья ЧелГУ по запросу обучающегося (мобильные специальные технические средства для лиц с нарушениями зрения и с нарушением слуха, ассистивные информационные технологии).

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

В учебные аудитории обеспечивается беспрепятственный доступ для обучающихся с инвалидностью и с ограниченными возможностями здоровья. В каждой аудитории, где обучаются инвалиды и лица с ограниченными возможностями здоровья, предусматривается соответствующее количество мест для обучающихся с учетом нарушений их здоровья.

Для освоения дисциплины инвалидам и лицам с ограниченными возможностями здоровья предоставляется доступ к печатным источникам, имеющимся в научной библиотеке ЧелГУ, с помощью специальных технических средств; доступ с помощью специальных технических и программных средств к электронным источникам, представленным в форме электронного документа в фонде научной библиотеки ЧелГУ или электронно-библиотечных системах.

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

Для инвалидов и лиц с ограниченными возможностями здоровья освоение дисциплины может быть частично или полностью осуществлено с использованием дистанционных образовательных технологий.

При проведении промежуточной аттестации по дисциплине обучающимся с инвалидностью и с ограниченными возможностями здоровья обеспечивается по их заявлению предоставление в доступной форме в зависимости от их индивидуальных особенностей инструкции о порядке проведения промежуточной аттестации, оценочных средств и возможности ответов на задания (письменно на бумаге, набор ответов на компьютере, письменно шрифтом Брайля, с использованием услуг ассистента, устно).

При проведении процедуры оценивания результатов обучения инвалидов и лиц с ограниченными возможностями здоровья предусматривается использование предоставленных ЧелГУ или собственных технических средств, необходимых им в связи с их индивидуальными особенностями. При необходимости инвалидам и лицам с ограниченными возможностями здоровья предоставляется дополнительное время для подготовки ответа на задания, процедура оценивания результатов обучения по дисциплине может проводиться в несколько этапов.